(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 748 834**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **96 06382**

(51) Int Cl⁶ : G 06 F 12/00, H 04 Q 7/32

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 17.05.96.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** 21.11.97 Bulletin 97/47.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS* — FR.

(72) **Inventeur(s) :** PROUST PHILIPPE, MOULINAS ANNE et HUET CEDRIC.

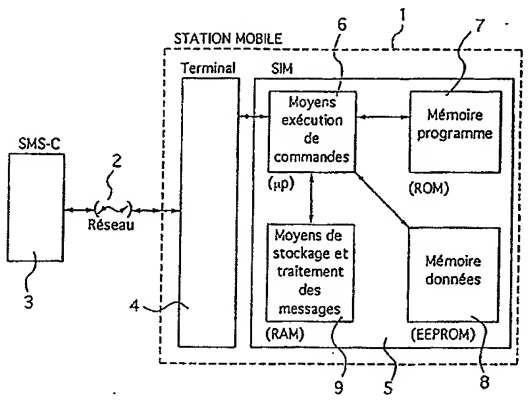
(73) **Titulaire(s) :** .

(74) **Mandataire :** CABINET PATRICE VIDON.

(54) SYSTEME DE COMMUNICATION PERMETTANT UNE GESTION SECURISEE ET INDEPENDANTE D'UNE PLURALITE D'APPLICATIONS PAR CHAQUE CARTE UTILISATEUR, CARTE UTILISATEUR ET PROCEDE DE GESTION CORRESPONDANTS.

(57) L'invention concerne un système de communication, du type comprenant notamment une pluralité d'équipements terminaux (1) constitués chacun d'un terminal (4) coopérant avec une carte utilisateur à microprocesseur (SIM; 5). Chaque carte utilisateur inclut des moyens (8) de mémorisation de données comprenant une pluralité d'objets et servant de support à au moins deux applications distinctes, la carte utilisateur comprenant des moyens (6, 7) d'exécution de commandes appartenant aux applications. Chaque objet compris dans les moyens de mémorisation de données d'une carte utilisateur est associé à une première politique de contrôle d'accès définie par un jeu de premières conditions d'accès.

Selon l'invention, chaque objet est également associé à au moins une autre politique de contrôle d'accès définie par un jeu d'au moins une condition d'accès alternative. Chaque condition d'accès alternative s'applique, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite autre politique de contrôle d'accès donnée. Chaque objet est également associé à une pluralité d'indicateurs de politique de contrôle d'accès indiquant chacun, pour une des applications, quelle politique de contrôle d'accès utiliser avec cette application, les indicateurs de politique de contrôle d'accès étant stockés dans les moyens (8) de mémorisation de données.



FR 2 748 834 - A1

Système de communication permettant une gestion sécurisée et indépendante d'une pluralité d'applications par chaque carte utilisateur, carte utilisateur et procédé de gestion correspondants.

Le domaine de l'invention est celui des systèmes de communication avec des équipements terminaux constitués chacun d'un terminal coopérant avec une carte utilisateur à microprocesseur.

L'invention s'applique notamment, mais non exclusivement, dans le cas d'un système de radiocommunication cellulaire avec des stations mobiles constituées chacune d'un terminal coopérant avec une carte utilisateur appelée module d'identification d'abonné (ou module SIM, pour "Subscriber Identity Module" en langue anglaise).

L'invention s'applique également, à nouveau non exclusivement, dans le cas d'un système de communication avec des stations de paiement constituées chacune d'un terminal bancaire coopérant avec une carte de paiement.

Plus précisément, l'invention concerne un système de communication permettant une gestion sécurisée et indépendante d'une pluralité d'applications par chaque carte utilisateur. L'invention concerne également une carte utilisateur et un procédé de gestion correspondants.

Les inconvénients des systèmes de communication connus sont présentés ci-dessous à travers l'exemple d'un système de radiocommunication cellulaire. Il est clair cependant que l'invention n'est pas limitée à ce type de système, mais concerne plus généralement tout système de communication dans lequel une carte utilisateur, destinée à coopérer avec un terminal, supporte plusieurs applications.

Dans le domaine de la radiocommunication cellulaire, on connaît notamment, principalement en Europe, le standard GSM ("Groupe spécial Systèmes Mobiles publics de radiocommunication fonctionnant dans la bande des 900 Mhz").

L'invention s'applique notamment, mais non exclusivement, à un système selon ce standard GSM. Plus généralement, elle peut s'appliquer à tous les systèmes dans lesquels chaque carte utilisateur peut gérer au moins deux applications distinctes.

Dans le cas d'un système de radiocommunication cellulaire, un terminal est un équipement physique utilisé par un usager du réseau pour accéder aux services de

télécommunication offerts. Il existe différents types de terminaux, tels que notamment les portatifs, les portables ou encore les mobiles montés sur des véhicules.

Quand un terminal est utilisé par un usager, ce dernier doit connecter au terminal sa carte utilisateur (module SIM), qui se présente généralement sous la forme d'une carte à puce.

La carte utilisateur supporte une application principale téléphonique (par exemple l'application GSM) qui permet son fonctionnement, ainsi que celui du terminal auquel elle est connectée, dans le système de radiocommunication cellulaire. Notamment, la carte utilisateur procure au terminal auquel elle est connectée un identifiant unique d'abonné (ou identifiant IMSI, pour "International Mobile Subscriber Identity" en langue anglaise). Pour cela, la carte utilisateur inclut des moyens d'exécution de commandes (par exemple, un microprocesseur et une mémoire programme) et des moyens de mémorisation de données (par exemple une mémoire de données).

L'identifiant IMSI, ainsi que toutes les informations individuelles concernant l'abonné et destinées à être utilisées par le terminal, sont stockées dans les moyens de mémorisation de données du module SIM. Ceci permet à chaque terminal d'être utilisé avec n'importe quel module SIM

Dans certains systèmes connus, et notamment dans un système GSM, il existe un service de messages courts (ou SMS, pour "Short Message Service" en langue anglaise) permettant l'envoi de messages courts vers les stations mobiles. Ces messages sont émis par un centre de service de messages courts (ou SMS-C, pour "SMS Center" en langue anglaise).

Lorsqu'une station mobile reçoit un message court, elle le stocke dans les moyens de mémorisation de données de son module SIM. L'application principale téléphonique de chaque module SIM de traiter chaque message court reçu.

A l'origine, l'unique fonction d'un message court était de fournir une information à l'abonné, généralement via un écran d'affichage du terminal. Les messages courts, dits messages courts normaux, qui remplissent cette unique fonction ne contiennent donc que des données brutes.

Par la suite, on a imaginé un service de messages courts amélioré (ou ESMS,

pour "Enhanced SMS" en langue anglaise), dans lequel deux types de messages courts peuvent être envoyés, à savoir les messages courts normaux précités et des messages courts améliorés pouvant contenir des commandes.

Ainsi, dans le document de brevet EP 562 890 par exemple, il est proposé de transmettre à un module SIM, via des messages courts améliorés, des commandes permettant de mettre à jour ou de reconfigurer ce module SIM à distance. En d'autres termes, des commandes encapsulées dans des messages courts améliorés permettent de modifier l'application principale téléphonique du module SIM.

On a également proposé que le module SIM serve de support à d'autres applications que l'application principale téléphonique, telles que notamment des applications de location de voiture, de paiement ou encore de fidélité.

Du fait que les commandes appartenant à ces autres applications sont contenues dans des messages courts améliorés, et donc externes au module SIM, ces autres applications sont dites distantes ou OTA (pour "Over The Air" en langue anglaise). Par opposition, l'application principale téléphonique, dont les commandes sont contenues dans les moyens de mémorisation de données du module SIM, est dite locale. Les commandes sont également dites locales ou distantes, selon que l'application à laquelle elles appartiennent est elle-même locale ou distante.

Le document de brevet PCT/GB/9401295 décrit par exemple un module SIM supportant les applications distantes suivantes : mise à jour de numéros de téléphones à distance, location (de voiture ou d'hôtel notamment) et paiement. Chaque message comprend une commande suivie de données. A titre d'exemple, les quatre types de commandes distantes suivants (parmi 255 possibles) sont présentés :

- les commandes d'écriture, permettant de stocker dans le module SIM, à partir d'un emplacement mémoire spécifié, des données contenues dans les messages reçus ;
- les commandes de lecture, permettant de lire des données dans le module SIM, à partir d'un emplacement mémoire spécifié, les données lues étant placées dans des messages à destination des appelants extérieurs ;
- les commandes de verrouillage/déverrouillage, permettant d'autoriser ou interdire

l'écriture et la lecture d'emplacements mémoires spécifiés du module SIM ;

- les commandes d'exécution de programme, permettant d'exécuter un programme stocké dans le module SIM.

Avec ces commandes distantes, on peut donc exécuter des applications distantes (location, paiement, reconfiguration de l'application principale téléphonique, ...). On peut également ajouter de nouvelles fonctionnalités au module SIM. Ainsi, le module SIM peut devenir une carte multiservice, avec par exemple les fonctionnalités d'une carte de crédit, d'un passeport, d'un permis de conduire, d'une carte de membre, etc.

Il est clair que ce récent concept de multi-application du module SIM est très avantageux pour l'abonné. En effet, ce dernier peut maintenant effectuer de façon très simple, uniquement avec un terminal dans lequel est inséré son module SIM, de nombreuses opérations telles que par exemple la location d'une voiture ou le paiement d'un service.

En revanche, ce récent concept de multi-application du module SIM, tel qu'il est mis en oeuvre actuellement, présente l'inconvénient majeur de ne pas assurer la gestion indépendante de chacune des applications, locale ou distante. En effet, dans tous les systèmes connus à ce jour, les fichiers des moyens de mémorisation de données du module SIM sont accessibles de la même façon par toutes les applications.

Ainsi, dans le document de brevet PCT/GB/9401295 précité, l'accès à certains emplacements mémoires par une commande est toujours autorisé, tandis que l'accès à d'autres emplacements mémoires par une commande peut être soit autorisé soit refusé. Mais, quel que soit l'emplacement mémoire concerné, l'accessibilité par une commande ne dépend en aucune façon de l'application à laquelle appartient cette commande.

De même, dans les spécifications GSM actuelles (et notamment la spécification GSM 11.11), aucune différence n'est faite entre les applications pour ce qui est des conditions d'accès aux fichiers des moyens de mémorisation de données du module SIM. En effet, chaque fichier possède sa propre politique de contrôle d'accès standard, qui est unique et définie par un jeu de conditions d'accès standard, chacune de ces conditions d'accès standard s'appliquant à une commande distincte pour ce fichier. Chaque condition d'accès standard peut prendre différentes valeurs, telles que par exemple

"ALWAYS" (accès toujours autorisé), "CHV1" ou "CHV2" (accès autorisé après vérification du possesseur du module SIM) et "NEVER" (accès jamais autorisé). Mais aucune de ces valeurs ne vise à lier l'accès au fichier à l'identité de l'application à laquelle appartient la commande qui demande cet accès.

Cette absence de contrôle de l'accès aux fichiers en fonction des applications n'est pas satisfaisante du point de vue sécurité. En effet, ceci signifie que toutes les applications distantes supportées par les moyens de mémorisation de données d'un même module SIM peuvent accéder à l'ensemble des fichiers de ces moyens de mémorisation de données. Rien n'empêche donc les données concernant une de ces applications distantes d'être lues ou même modifiées par une autre de ces applications distantes. Il ressort clairement de ce qui précède que chaque application distante ne dispose pas pour ses données propres stockées dans le module SIM d'une sécurité et d'une confidentialité suffisantes.

L'invention a notamment pour objectif de pallier cet inconvénient majeur de l'état de la technique.

Plus précisément, l'un des objectifs de la présente invention est de fournir un système de communication (et notamment, mais non exclusivement, un système de radiocommunication cellulaire) dans lequel chaque carte utilisateur peut gérer de façon sécurisée et indépendante une pluralité d'applications.

En d'autres termes, l'un des objectifs de l'invention est de permettre à chaque fournisseur d'application d'éviter que d'autres applications que la sienne puissent accéder à au moins certains des objets (par exemple des fichiers) de la carte utilisateur qui supportent son application.

Un autre objectif de l'invention est de permettre la mise à jour (ou la reconfiguration) des objets de la carte utilisateur qui supportent les différentes applications, tout en s'assurant que ces applications continuent à être gérées de façon sécurisée et indépendante.

Un objectif complémentaire de l'invention est de permettre la création à distance d'une nouvelle application qui, comme les applications déjà existantes, est supportée par des objets dont au moins certains auxquels elle est seule à pouvoir accéder.

Ces différents objectifs, ainsi que d'autres qui apparaîtront par la suite, sont atteints selon l'invention à l'aide d'un système de communication, du type comprenant notamment une pluralité d'équipements terminaux constitués chacun d'un terminal coopérant avec une carte utilisateur à microprocesseur,

chaque carte utilisateur incluant des moyens de mémorisation de données comprenant une pluralité d'objets, lesdits moyens de mémorisation de données servant de support à au moins deux applications distinctes, ladite carte utilisateur comprenant des moyens d'exécution de commandes appartenant auxdites applications,

chaque objet compris dans les moyens de mémorisation de données d'une carte utilisateur étant associé à une première politique de contrôle d'accès définie par un jeu de premières conditions d'accès, chacune desdites premières conditions d'accès s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite première politique de contrôle d'accès,

caractérisé en ce que chaque objet est également associé à au moins une autre politique de contrôle d'accès, chaque autre politique de contrôle d'accès étant définie par un jeu d'au moins une condition d'accès alternative, chaque condition d'accès alternative d'une autre politique de contrôle d'accès donnée s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite autre politique de contrôle d'accès donnée,

et en ce que chaque objet est également associé à une pluralité d'indicateurs de politique de contrôle d'accès, chaque indicateur de politique de contrôle d'accès indiquant, pour une desdites applications, quelle politique de contrôle d'accès, à savoir première ou autre, utiliser avec cette application, lesdits indicateurs de politique de contrôle d'accès étant stockés dans lesdits moyens de mémorisation de données.

Le principe général de l'invention consiste donc à :

- associer à chaque objet (qui est par exemple un fichier), en plus de la première politique de contrôle d'accès (dite dans certains cas "standard"), une ou plusieurs autres politiques de contrôle d'accès ; et
- indiquer, pour chaque objet, la politique de contrôle d'accès (première ou autre) à utiliser avec chaque application.

Ainsi, l'accès à l'objet (par une commande) peut ne pas être identique pour toutes les applications. Chaque application voit l'accès de ses différentes commandes à un objet définit par celles des politiques de contrôle d'accès qui lui est associée pour cet objet.

Avantageusement, pour chaque objet, au moins une autre politique de contrôle d'accès est spécifique à une des applications, chaque condition d'accès alternative de cette autre politique de contrôle d'accès spécifique s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à l'unique application utilisant cette autre politique de contrôle d'accès spécifique.

De façon avantageuse, pour chaque objet, au moins une autre politique de contrôle d'accès est entièrement commune à au moins deux applications, chaque condition d'accès alternative de cette autre politique de contrôle d'accès entièrement commune s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant auxdites au moins deux applications utilisant cette autre politique de contrôle d'accès entièrement commune.

Avantageusement, pour chaque objet, au moins une autre politique de contrôle d'accès est partiellement commune à au moins deux applications,

certaines des conditions d'accès alternatives de cette autre politique de contrôle d'accès partiellement commune s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant auxdites au moins deux applications utilisant cette autre politique de contrôle d'accès commune,

d'autres des conditions d'accès alternatives de cette autre politique de contrôle d'accès partiellement commune s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant uniquement à l'une desdites au moins deux applications utilisant cette autre politique de contrôle d'accès commune.

Ainsi, pour chaque objet, chaque application peut :

- soit avoir son propre jeu de conditions d'accès alternatives ;
- soit partager tout son jeu de conditions d'accès alternatives avec une ou plusieurs autres applications ;
- soit partager une partie seulement de son jeu de conditions d'accès alternatives avec une ou plusieurs autres applications.

Dans le cas le plus simple, chaque objet est associé d'une part à la première politique de contrôle d'accès et d'autre part à une unique autre politique de contrôle d'accès. Cette dernière est définie par une seule condition d'accès, s'appliquant de façon commune à toutes les commandes des applications qui l'utilisent.

Dans le cas le plus complexe, chaque objet est associé d'une part à la première politique de contrôle d'accès et d'autre part à autant d'autres politiques de contrôle d'accès distinctes qu'il existe d'applications. Chacune de ces autres politiques de contrôle d'accès est définie par une pluralité de conditions d'accès distinctes s'appliquant chacune à une seule ou plusieurs des commandes appartenant à cette autre politique de contrôle d'accès.

Dans un mode de réalisation particulier du système de l'invention, du type permettant une radiocommunication cellulaire, ladite pluralité d'équipements terminaux est une pluralité de stations mobiles, lesdites cartes utilisateur étant des modules d'identification d'abonné.

Dans ce cas particulier d'un système de radiocommunication cellulaire, la pluralité d'applications supportées par les moyens de mémorisation de la carte utilisateur comprend par exemple l'application principale téléphonique (par exemple l'application GSM) et :

- soit au moins une application distante (par exemple de location de voiture, de paiement ou encore de fidélité), dont les commandes sont fournies à partir de l'extérieur aux moyens d'exécution de commande de la carte utilisateur (par exemple via des messages courts améliorés) ; et
- soit au moins une autre application locale, dont les commandes sont fournies en interne aux moyens d'exécution de commande de la carte utilisateur (par exemple à partir d'une mémoire programme ROM de cette carte utilisateur).

Il est à noter que la première situation est plus fréquente que la seconde, du fait qu'une carte utilisateur ne supporte généralement qu'une application locale, à savoir l'application principale téléphonique. Cependant, la seconde situation peut également être envisagée.

Ainsi, selon l'invention, dans le cas particulier d'un système de radiocommunication cellulaire, chaque carte utilisateur peut gérer de façon sécurisée et indépendante toutes ou certaines des applications qu'il supporte.

Dans un mode de réalisation avantageux de l'invention, ledit système étant du type comprenant en outre au moins un centre de service de messages,

lesdits moyens de mémorisation de données d'une carte utilisateur servant de support à au moins une application locale et au moins une application distante de ladite carte utilisateur, les commandes étant dites locales, lorsqu'elles appartiennent à ladite application locale, ou distantes, lorsqu'elles appartiennent à ladite application distante,

chaque terminal pouvant recevoir des messages, de type normal ou amélioré, émis par ledit centre de service de messages, chaque carte utilisateur comprenant des moyens de stockage et de traitement des messages reçus par le terminal avec lequel elle coopère,

les messages normaux contenant des données brutes constituant une information destinée à être fournie à l'abonné via notamment un écran d'affichage du terminal, les messages améliorés contenant des commandes distantes,

ledit système est caractérisé en ce que lesdits moyens de mémorisation de données de chaque carte utilisateur stockent également une liste d'applications distantes autorisées,

et en ce que chaque carte utilisateur comprend également des moyens de discrimination des messages améliorés, permettant de bloquer chaque message amélioré qui contient des commandes distantes n'appartenant pas à une desdites applications distantes autorisées.

Ainsi, la carte utilisateur détecte si l'application distante émettrice du message amélioré est autorisée à accéder à cette carte utilisateur. Cette opération de discrimination constitue un niveau de sécurité supplémentaire pour l'accès des commandes à la mémoire de données de la carte utilisateur.

Les messages normaux ou améliorés sont par exemple des messages courts, selon le vocabulaire GSM.

De façon préférentielle, lesdits moyens de mémorisation de données de chaque carte utilisateur stockent également, pour chacune desdites applications distantes autorisées, une référence secrète et un mode d'authentification de message associés,

et chaque carte utilisateur comprend également des moyens d'authentification des messages améliorés discriminés, permettant d'authentifier un message amélioré discriminé en utilisant la référence secrète et le mode d'authentification de message associés, dans lesdits moyens de mémorisation de données, à l'application distante autorisée à laquelle appartiennent les commandes contenues dans ledit message amélioré discriminé.

En d'autres termes, la carte utilisateur authentifie chaque message amélioré discriminé selon le mode d'authentification et la référence secrète associés à l'application émettrice de ce message. Cette opération d'authentification constitue encore un autre niveau de sécurité supplémentaire pour l'accès des commandes à la mémoire de données de la carte utilisateur.

Avantageusement, pour chaque objet, la ou au moins une des autres politiques de contrôle d'accès, dite seconde politique de contrôle d'accès, est définie par un jeu d'au moins une condition d'accès alternative particulière, chaque condition d'accès alternative particulière pouvant prendre notamment les valeurs suivantes :

- "aucun accès" : si ledit objet n'est accessible par aucune commande dudit groupe d'au moins une commande auquel s'applique ladite condition d'accès alternative particulière ;
- "accès privé" : si ledit objet n'est accessible que par les commandes appartenant à une unique application prédéterminée, parmi ledit groupe d'au moins une commande auquel s'applique ladite condition d'accès alternative particulière ;
- "accès partagé" : si ledit objet est accessible par les commandes appartenant à au moins deux applications prédéterminées, parmi ledit groupe d'au moins une commande auquel s'applique ladite condition d'accès alternative particulière.

Dans un mode de réalisation particulier de l'invention, pour chaque objet, au moins une autre politique de contrôle d'accès, dite politique de contrôle d'accès à distance, est définie par un jeu d'au moins une condition d'accès à distance, chaque condition d'accès à distance s'appliquant, pour ledit objet, à un groupe d'au moins une

commande distante appartenant à la ou aux applications distantes utilisant ladite politique de contrôle d'accès à distance,

et pour chaque objet, seuls les indicateurs de politique de contrôle d'accès associés chacun à une des applications distantes peuvent indiquer ladite politique de contrôle d'accès à distance.

Dans ce mode de réalisation particulier, chaque objet peut voir son accès autorisé ou interdit à chaque application distante, à condition bien sûr que la politique de contrôle d'accès à distance soit celle devant effectivement être utilisée avec cette application distante.

Pour chaque objet, on peut prévoir :

- soit une politique de contrôle d'accès à distance distincte pour chaque application distante ;
- soit une même politique de contrôle d'accès à distance pour au moins certaines des applications distantes (ou bien pour toutes).

Il est à noter que si, mise à part la première politique de contrôle d'accès, l'unique ou toutes les autres politiques de contrôle d'accès sont des politiques de contrôle d'accès à distance, alors la première politique de contrôle d'accès doit obligatoirement être utilisée avec la ou les applications locales.

De façon avantageuse, pour chaque objet, chaque condition d'accès à distance peut prendre les mêmes valeurs que lesdites conditions d'accès alternatives particulières.

Ainsi, il est possible de réaliser une partition de la mémoire de données de la carte utilisateur entre les différentes applications distantes. En effet, certains objets peuvent être rendus accessibles :

- soit ("aucun accès") par aucune commande distante, quelle que soit l'application distante à laquelle cette commande distante appartient ;
- soit ("accès privé") seulement par toutes ou certaines des commandes appartenant à une unique application distante, dite parente de cet objet ;
- soit ("accès partagé") par toutes ou certaines des commandes appartenant à certaines applications distantes bien déterminées.

De cette façon, tous les objets à accès privé liés à une même application distante

parente constituent une zone sécurisée et étanche, propre à cette application parente et inaccessible aux autres applications. Le fournisseur d'une application distante donnée est ainsi assuré que d'autres applications distantes que la sienne ne peuvent pas accéder à la zone sécurisée qui lui est allouée.

Dans un mode de réalisation avantageux de l'invention, dans lequel lesdits moyens de mémorisation de données de chaque carte utilisateur sont du type possèdant une structure hiérarchique à au moins trois niveaux et comprenant au moins les trois types de fichiers suivants :

- fichier maître, ou répertoire principal ;
- fichier spécialisé, ou répertoire secondaire placé sous ledit fichier maître ;
- fichier élémentaire, placé sous un desdits fichiers spécialisés, dit fichier spécialisé parent, ou directement sous ledit fichier maître, dit fichier maître parent,

ledit système est caractérisé en ce que lesdits moyens de mémorisation de données de chaque carte utilisateur comprennent au moins un fichier élémentaire système, chaque fichier élémentaire système étant lié à une application distante autorisée et stockant une première information de localisation de la référence secrète et du mode d'authentification de message associés à cette application distante autorisée à laquelle il est lié,

et en ce que chaque message amélioré comprend une seconde information de localisation du fichier élémentaire système auquel est liée l'application distante autorisée à laquelle appartiennent les commandes contenues dans ledit message amélioré,

lesdits moyens d'authentification lisant dans chaque message amélioré discriminé ladite seconde information de localisation du fichier élémentaire système, de façon à lire dans le fichier élémentaire système ladite première information de localisation de la référence secrète et du mode d'authentification de message à utiliser pour authentifier ledit message amélioré discriminé.

Ainsi, chaque fichier élémentaire système contient des informations permettant de retrouver les éléments nécessaire à l'opération d'authentification d'un message émis par l'application distante à laquelle est lié ce fichier élémentaire système. De son côté, chaque message comporte (dans son en-tête) des informations permettant de retouver le fichier

élémentaire système auquel son application émettrice est liée, de façon que son authentification puisse être effectuée.

Avantageusement, chaque fichier élémentaire système est placé sous un fichier spécialisé ou directement sous le fichier maître, un fichier élémentaire système au maximum pouvant être placé sous chaque fichier spécialisé, et un fichier élémentaire système au maximum pouvant être placé directement sous le fichier maître.

De façon préférentielle, si aucun fichier élémentaire système n'existe sous un fichier spécialisé, ni sous le fichier maître, alors chaque fichier élémentaire placé sous ledit fichier spécialisé, quelle que soit la valeur des conditions d'accès à distance associées à ce fichier élémentaire, n'est accessible par aucune commande distante,

et si aucun fichier élémentaire système n'existe directement sous le fichier maître, alors chaque fichier élémentaire placé directement sous le fichier maître, quelle que soit la valeur des conditions d'accès à distance associées à ce fichier élémentaire, n'est accessible par aucune commande distante.

Ceci signifie que pour être accessible par une commande distante, un fichier doit être placé sous un fichier spécialisé ou directement sous un fichier maître auquel se rapporte un fichier élémentaire système. Ce qu'on entend ici par "se rapporte" est précisé par la suite.

Préférentiellement, ladite seconde information de localisation du fichier élémentaire système est un identificateur d'un fichier spécialisé ou d'un fichier maître auquel se rapporte ledit fichier élémentaire système selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

Avantageusement, ladite stratégie de recherche prédéterminée dans les moyens de mémorisation de données est un mécanisme de recherche en amont (du type "backtracking"), consistant à rechercher si un fichier élémentaire système existe sous le fichier spécialisé ou le fichier maître indiqué par ledit identificateur, et, dans la négative et si l'identificateur n'indique pas le fichier maître, à rechercher si un fichier élémentaire système existe directement sous le fichier maître.

Ainsi, l'expression "se rapporte" utilisée précédemment correspond par exemple à une recherche de type "backtracking".

Dans un mode de réalisation avantageux de l'invention, dans le cas d'un fichier dont une des conditions d'accès à distance possède la valeur "accès privé", ladite unique application distante prédéterminée dont les commandes distantes peuvent accéder audit fichier est, sous réserve que son authentification soit réussie, l'application distante autorisée parente dudit fichier, c'est-à-dire l'application distante autorisée liée au même fichier élémentaire système que celui auquel se rapporte le fichier spécialisé parent ou le fichier maître parent dudit fichier,

et, dans le cas d'un fichier dont la condition d'accès à distance possède la valeur "accès partagé", lesdites au moins deux applications distantes prédéterminées dont les commandes distantes peuvent accéder audit fichier sont, sous réserve que leur authentification soit réussie, toutes les applications distantes autorisées, quel que soit le fichier élémentaire système auquel chacune d'elles est liée.

Ainsi, une application parente liée à un fichier élémentaire système donné a comme fichiers enfants tous les fichiers dont le fichier spécialisé parent ou le fichier maître parent (c'est-à-dire le fichier spécialisé ou le fichier maître sous lequel ils sont directement placés) se rapporte à ce fichier élémentaire système donné.

L'ensemble des fichiers enfants d'une application parente constitue un regroupement logique de fichiers, également appelé domaine de sécurité propre à cette application. Dans le cas d'un accès distant autorisé du type "privé", c'est ce domaine de sécurité qui délimite la zone sécurisée spécifique à l'application bénéficiant de ce droit privatif.

En d'autres termes, le domaine de sécurité consiste pour partie à regrouper logiquement les fichiers en fonction de leur lien de dépendance parent/enfant avec une application. Chaque application possède son domaine de sécurité. Cela consiste en fait à donner une définition des objets du domaine de sécurité de l'application. Le regroupement logique des fichiers peut donc être appelé domaine de sécurité de l'application, ou encore domaine de validité du schéma sécuritaire de l'application.

De façon avantageuse, chaque fichier élémentaire système comprend un ensemble distinct d'indicateurs de politique de contrôle d'accès, chaque indicateur de politique de contrôle d'accès indiquant, pour une desdites applications, quelle politique de contrôle

d'accès, à savoir première ou autre, utiliser avec cette application,

ledit ensemble distinct d'indicateurs de politique de contrôle d'accès étant associé à tous les fichiers dont le fichier spécialisé parent ou le fichier maître parent se rapporte audit fichier élémentaire système.

L'invention concerne également une carte utilisateur à microprocesseur du type destiné à coopérer avec un terminal de façon à constituer un équipement terminal d'un système de communication tel que précité,

caractérisée en ce que chaque objet des moyens de mémorisation de données de ladite carte utilisateur est également associé à au moins une autre politique de contrôle d'accès, chaque autre politique de contrôle d'accès étant définie par un jeu d'au moins une condition d'accès alternative, chaque condition d'accès alternative d'une autre politique de contrôle d'accès donnée s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite autre politique de contrôle d'accès donnée,

et en ce que chaque objet est également associé à une pluralité d'indicateurs de politique de contrôle d'accès, chaque indicateur de politique de contrôle d'accès indiquant, pour une desdites applications, quelle politique de contrôle d'accès, à savoir première ou autre, utiliser avec cette application, lesdits indicateurs de politique de contrôle d'accès étant stockés dans les moyens de mémorisation de données de ladite carte utilisateur.

L'invention concerne aussi un procédé de gestion sécurisée et indépendante d'au moins deux applications distantes, par une carte utilisateur à microprocesseur du type destiné à coopérer avec un terminal de façon à constituer un équipement terminal d'un système de communication tel que précité,

caractérisé en ce que, pour chaque message amélioré reçu, ladite carte utilisateur effectue notamment l'étape suivante : pour chaque commande distante contenue dans ledit message amélioré, vérification de l'accessibilité de cette commande distante à l'objet concerné, ladite vérification de l'accessibilté s'appuyant sur une politique de contrôle d'accès, première ou à distance, à utiliser pour ledit objet concerné avec ladite application distante courante.

Avantageusement, pour chaque message amélioré reçu, ladite carte utilisateur effectue également une étape préalable de discrimination dudit message amélioré, de façon à ne poursuivre son traitement que si l'application distante, dite application distante courante, à laquelle appartiennent les commandes distantes qu'il contient est une application distante autorisée.

De façon avantageuse, pour chaque message amélioré reçu, ladite carte utilisateur effectue également une étape préalable d'authentification dudit message amélioré, en utilisant une référence secrète et un mode d'authentification de message associés à ladite application distante courante.

Avantageusement, au moins certains des éléments appartenant au groupe suivant peuvent être créés et/ou mis à jour et/ou supprimés par l'intermédiaire de commandes distantes :

- les valeurs des conditions d'accès, notamment premières ou à distance, des politiques de contrôle d'accès associées à chaque objet ;
- l'indicateur de politique de contrôle d'accès, notamment première ou à distance, à utiliser avec chaque application pour chaque objet ;
- la liste des applications distantes autorisées ;
- pour chacune des applications distantes autorisées de ladite liste, la référence secrète et le mode d'authentification de message associés ;
- le ou lesdits fichiers élémentaires système liés chacun à une application distante autorisée distincte ;
- les fichiers élémentaires, spécialisé et maître.

Ainsi, la sécurisation d'accès aux objets selon l'invention peut être adaptée, par mise à jour ou reconfiguration, à l'évolution des besoins de chaque application.

De plus, des applications (par exemple distantes) entièrement nouvelles peuvent être ajoutées et supportées par la mémoire de données de la carte mémoire. Ces nouvelles applications (distantes) peuvent bénéficier, de la même façon que les applications (distantes) prévues à l'origine, d'une sécurité d'accès propre (avec par exemple un mode d'authentification, une référence secrète et un schéma sécuritaire spécifiques).

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la

description suivante d'un mode de réalisation préférentiel de l'invention, donné à titre d'exemple indicatif et non limitatif, et des dessins annexés, dans lesquels :

- la figure 1 présente un schéma synoptique simplifié d'un mode de réalisation particulier d'un système de radiocommunication cellulaire selon l'invention ;
- la figure 2 présente la structure d'un mode de réalisation particulier d'un message court amélioré selon l'invention reçu par le module SIM de la figure 1 ;
- la figure 3A présente de façon schématique un mode de réalisation particulier d'un fichier de la mémoire de données de la figure 1, avec ses politiques de contrôle d'accès et ses indicateurs associés ;
- la figure 3B présente un exemple d'une pluralité d'indicateurs tels qu'associés à un fichier comme présenté sur la figure 3A ;
- la figure 4 présente un premier exemple de partition de la mémoire de données de la figure 1 entre plusieurs applications ;
- la figure 5 présente un organigramme simplifié d'un mode de réalisation particulier du traitement par le module SIM de la figure 1 d'un message court amélioré ;
- les figures 6 et 7 permettent d'expliciter les étapes de filtrage d'application et d'authentification de message apparaissant sur la figure 5 ;
- les figures 8 et 9 permettent d'expliciter l'étape de sécurisation de l'exécution d'une commande apparaissant sur la figure 5 ;
- la figure 10 présente un second exemple de partition de la mémoire de données de la figure 1 entre plusieurs applications.

Dans le mode de réalisation particulier décrit ci-dessous, uniquement à titre d'exemple, le système de communication est un système de radiocommunication cellulaire du type GSM. Il est clair toutefois que l'invention n'est pas limitée à ce type particulier de système de communication, mais concerne plus généralement tous les systèmes de communication comprenant une pluralité d'équipements terminaux constitués chacun d'un terminal coopérant avec une carte utilisateur à microprocesseur.

Dans un souci de simplification, sur la figure 1, on a représenté uniquement une station mobile (MS) 1 reliée, via un réseau 2, à un centre de service de messages courts (SMS-C) 3. En réalité, le système comprend une pluralité de stations mobiles 1, constituées chacune d'un terminal (ME) 4 coopérant avec un module d'identification d'abonné (module SIM) 5.

Chaque module SIM 5 comprend notamment, de façon classique :

- des moyens 6 d'exécution de commandes, constitués généralement d'un microprocesseur ;
- une mémoire programme 7, stockant l'application GSM (ou plus généralement l'application principale téléphonique) et éventuellement d'autres applications locales. Cette mémoire programme 7 est par exemple une mémoire ROM ;
- une mémoire de données 8, servant de support à toutes les applications, locales ou distantes, que le module SIM peut exécuter. En d'autres termes, elle stocke toutes les données auxquelles les applications supportées doivent pouvoir accéder lors de leur exécution. Par exemple, elle stocke toutes les informations individuelles de l'abonné (telles que notamment son numéro international d'abonné (identifiant IMSI), sa clé d'authentification individuelle (Ki) et l'algorithme d'authentification (A3)) nécessaires à l'exécution de l'application GSM. Cette mémoire de données 8 est par exemple une mémoire EEPROM ;
- des moyens 9 de stockage et traitement des messages courts reçus. En effet, chaque message court reçu par le terminal 4 est transmis au module SIM 5 pour traitement par l'application GSM.

Le SMS-C 3 met en oeuvre un service de messages courts amélioré (ESMS) qui permet d'envoyer deux types de messages courts à l'ensemble des stations mobiles 1, à savoir :

- des messages courts "normaux", qui transportent uniquement des données brutes. Les données brutes d'un message court normal correspondent à une information à afficher sur un écran du terminal 4, par exemple pour

inviter l'abonné à rappeler un numéro donné ;

- des messages courts "améliorés", qui transportent des commandes appartenant à des applications dites distantes (ou OTA), du fait que les commandes (également dites distantes) qui les constituent ne sont pas stockées dans la mémoire programme 7 du module SIM.

La figure 2 présente la structure d'un mode de réalisation particulier d'un message court amélioré selon l'invention reçu par le module SIM 5. Ce message court amélioré 20 comprend un en-tête SMS 21 (SMS Header en langue anglaise) et un corps 22 (TP-UD, pour "Transfer layer Protocol - User Data" en langue anglaise). Les commandes distantes Cmd1, Cmd2, etc sont placées dans le corps 22. Il s'agit par exemple de commandes classiques (opérationnelles ou administratives), définies dans les normes GSM 11.11, ISO 78.16-4 ou encore EN 726-3, telles que SELECT, UPDATE BINARY, UPDATE RECORD, SEEK, CREATE FILE, CREATE RECORD, EXTEND, etc. Les autres champs concernés par la présente invention sont présentés en détail dans la suite de la description.

La mémoire de données 8 comprend une pluralité de fichiers. De façon classique, et comme spécifié dans la norme GSM 11.11, chacun de ces fichiers est associé à une politique de contrôle d'accès standard. Celle-ci est définie par une pluralité de conditions d'accès standard (Standard AC) s'appliquant chacune à une commande distincte susceptible d'accéder à ce fichier. Chaque condition d'accès standard peut prendre différentes valeurs (par exemple "ALWays", "CHV1", "CHV2" ou encore "NEVer"). Aucune de ces valeurs n'est fonction de l'application à laquelle appartient la commande qui désire accéder au fichier.

Le principe général de l'invention consiste à associer également à chaque fichier de la mémoire de données 8 :

- au moins une autre politique de contrôle d'accès, chaque autre politique de contrôle d'accès étant définie par un jeu d'au moins une condition d'accès alternative, chaque condition d'accès alternative d'une autre politique de contrôle d'accès donnée s'appliquant, pour ce fichier, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant cette

autre politique de contrôle d'accès ; et

- pour chacune des applications supportées, un indicateur de politique de contrôle d'accès, indiquant quelle politique de contrôle d'accès, à savoir standard ou autre, utiliser avec cette application.

Dans un souci de simplification, dans l'exemple présenté dans la suite de la description, les applications ne possèdent pas chacune, pour chaque fichier, une autre politique de contrôle d'accès qui leur est propre (avec leur propre jeu de conditions d'accès alternatives) mais se partagent toutes, et de façon complète (c'est-à-dire pour toutes leurs commandes sans distinction), deux autres politiques de contrôles d'accès communes (avec chacune une unique condition d'accès qui s'applique pour toutes les commandes).

La figure 3A présente de façon schématique un mode de réalisation particulier d'un fichier 30 de la mémoire de données 8, avec ses politiques de contrôle d'accès 31 et ses indicateurs associés 32. Le tableau de l'annexe 1 présente un exemple d'une pluralité de politiques de contrôle d'accès telles qu'associées à ce fichier 30. La figure 3B présente un exemple d'une pluralité d'indicateurs 32 tels qu'associés au fichier 30.

Dans l'exemple suivant de caractéristiques associées à un fichier 30, décrit en relation avec la figure 3B et le tableau de l'annexe 1, on considère que :

- le module SIM supporte l'application GSM (unique application locale) et trois applications distantes (appli. dist. 1, appli. dist. 1' et appli. dist. 1'') ;
- il existe une politique de contrôle d'accès standard (PCA standard) et deux politiques de contrôle d'accès à distance (PCA à distance n°1 et PCA à distance n°2).

Comme présenté sur le tableau de l'annexe 1, dans la politique de contrôle d'accès standard, chaque commande (distante ou locale), quelle que soit l'application à laquelle elle appartient (application GSM ou l'une des applications distantes), est associée à une condition d'accès standard spécifique (cond. d'accès std 1, cond. d'accès std 2, ...). De façon classique, chaque condition d'accès standard possède une valeur appartenant au groupe comprenant : "ALWAYS" (accès toujours autorisé), "CHV1" ou "CHV2" (accès

autorisé après vérification du possesseur du module SIM) et "NEVER" (accès jamais autorisé).

Dans la politique de contrôle d'accès à distance n°1, toutes les commandes distantes (dans un souci de simplification), quelle que soit l'application à laquelle elles appartiennent, sont associées à une même condition d'accès à distance (également dans un souci de simplification) (cond. d'accès à dist. 1). Cette condition d'accès à distance peut par exemple prendre l'une des trois valeurs suivantes : "PARTAGE", "PRIVE" et "JAMAIS". Ainsi, dans cet exemple, elle possède la valeur "PARTAGE".

On explique maintenant le sens de chacune de ces trois valeurs :

- "JAMAIS" (ou "aucun accès") signifie que le fichier 30 n'est accessible par aucune commande, quelle que soit l'application à laquelle appartient cette commande ;
- "PRIVE" (ou "accès privé") signifie que le fichier 30 n'est accessible que par les commandes appartenant à une unique application prédéterminée ;
- "PARTAGE" (ou "accès partagé") signifie que le fichier 30 est accessible par les commandes appartenant à au moins deux applications prédéterminées.

On notera que les trois valeurs "PARTAGE", "PRIVE" et "JAMAIS" sont encore discutées dans la suite de la description, en relation avec les figures 9 à 11.

Dans la politique de contrôle d'accès à distance n°2, toutes les commandes distantes, quelle que soit l'application à laquelle elles appartiennent, sont associées à une même condition d'accès à distance (cond. d'accès à dist. 2). Cette condition d'accès à distance peut par exemple prendre une valeur X parmi un autre groupe de valeurs (X, Y, Z, ...) que celui précité (et comprenant les valeurs "PARTAGE", "PRIVE" et "JAMAIS").

Comme présenté sur la figure 3B, pour chacune des applications supportées (appli. GSM, appli. dist. 1, appli. dist. 1' et appli. dist. 1'') , un indicateur de politique de contrôle d'accès précise quelle politique de contrôle d'accès utiliser avec cette application (à savoir PCA standard, PCA à distance n°1 ou PCA à distance n°2).

Ainsi, on peut obtenir une partition de la mémoire de données 8 (et plus

précisément de l'ensemble des fichiers utilisant une même politique de contrôle d'accès à distance) en fonction des différentes applications distantes suppportées par cette mémoire de données.

Dans l'exemple présenté sur la figure 4, tous les fichiers de la mémoire de données utilisent la politique de contrôle d'accès à distance n°1. Ainsi, vu de l'extérieur (c'est-à-dire pour les applications distantes), la mémoire de données apparaît partagée entre une application locale et trois applications distantes (Fidélité, Paiement et GSM). On notera que, dans cet exemple, l'application appélée GSM n'est pas locale mais distante.

La mémoire de données 8 possède, dans le mode de réalisation présenté à titre d'exemple, une structure hiérarchique à trois niveaux et comprend les trois types de fichiers suivants :

- un fichier maître (MF), ou répertoire principal ;
- une pluralité de fichiers spécialisés (DF, $DF_{Fidélité}$, $DF_{Paiement}$, DF_{GSM}, $DF_{Télécom}$), qui sont des répertoires secondaires placés sous le fichier maître ;
- une pluralité de fichiers élémentaires (EF), placés chacun soit sous un des fichiers spécialisés (dit alors fichier spécialisé parent) soit directement sous le fichier maître (dit alors fichier maître parent).

On distingue huit groupes de fichiers, à savoir :

- groupe A : les fichiers uniquement accessibles par les commandes de l'application distante Fidélité, c'est-à-dire les fichiers dont la condition d'accès à distance est "PRIVE" pour l'application Fidélité ;
- groupe B : les fichiers uniquement accessibles par les commandes de l'application distante Paiement ;
- groupe C : les fichiers accessibles par les commandes des applications distantes Fidélité et Paiement, c'est-à-dire les fichiers dont la condition d'accès à distance est "PARTAGE" pour les applications Fidélité et Paiement ;
- groupe D : les fichiers uniquement accessibles par les commandes de l'application distante Télécom ;

- groupe E : les fichiers accessibles par les commandes des applications distantes Télécom et Fidélité ;
- groupe F : les fichiers accessibles par les commandes des applications distantes Paiement et Fidélité ;
- groupe G : les fichiers accessibles par les commandes des applications distantes Télécom, Paiement et Fidélité ;
- groupe H : les fichiers accessibles par les commandes d'aucune application distante, c'est-à-dire les fichiers dont la condition d'accès à distance est "JAMAIS".

Il est à noter que les fichiers du groupe H restent accessibles aux commandes de l'application locale (sous réserve que les conditions d'accès standard correspondantes soient vérifiées). De même, les fichiers du groupe H seraient accessibles aux commandes d'applications distantes qui utiliseraient la politique de contrôle d'accès standard et non pas la politique de contrôle d'accès à distance (sous réserve là encore que les conditions d'accès standard correspondantes soient vérifiées).

On présente maintenant, en relation avec l'organigramme de la figure 5, un mode de réalisation particulier du procédé de traitement par le module SIM d'un message court amélioré. Pour chaque message court amélioré reçu, le module SIM effectue notamment les étapes suivantes :

- il détermine (51) si le message court reçu (également appelé signal OTA) est un message court amélioré (et contient donc des commandes appartenant à une application distante) ou un message court normal ;
- il poursuit (52) le traitement s'il s'agit d'un message court amélioré, et l'interrompt (53) dans le cas contraire ;
- il détermine (54) si l'application distante émettrice du message (c'est-à-dire l'application dont des commandes sont contenues dans le message) est une application distante autorisée (étape 54 de discrimination d'application) ;
- il poursuit (55) le traitement s'il s'agit d'une application distante autorisée, et l'interrompt (56) dans le cas contraire ;
- il vérifie (57) l'authenticité du message en utilisant une référence secrète et un

mode d'authentification de message associés à l'application distante émettrice du message (étape 57 d'authentification de message) ;

- il poursuit (58) le traitement s'il l'authentification est correcte, et l'interrompt (59) dans le cas contraire ;
- pour chaque commande distante contenue dans le message :
  * il interprète (510) chaque commande distante (également appelée opération) contenue dans le message ;
  * il vérifie (511) l'accessibilité de cette commande distante au fichier concerné (également appelé champ de données), en fonction de la politique de contrôle d'accès, standard ou à distance, à utiliser pour le fichier concerné avec l'application distante émettrice du message (étape 511 de sécurisation de l'exécution d'une commande) ;
  * il poursuit (512) le traitement si la commande distante peut accéder au fichier, et passe (513) dans le cas contraire à l'étape 515 d'établissement d'un compte-rendu ;
  * il exécute (514) la commande ; et
- il établit (515) un compte-rendu d'exécution.

Les figures 6, 7 et 8 permettent d'expliciter les étapes de discrimination d'application 54 et d'authentification de message 57.

Comme présenté sur la figure 6, un fichier 60 de la mémoire de données 8 stocke une liste d'applications distantes autorisées. Ce fichier 60, appelé fichier élémentaire d'entrée (ou encore EF SMS Log), contient par exemple les adresses (TP-OA 1 à TP-OA n) de chacun des fournisseurs d'application distante autorisée. Ces adresses sont appelées adresses TP-OA, pour "TP-Originating-Addresses" en langue anglaise. Par ailleurs, chaque message court amélioré comprend dans son en-tête (cf figure 2) un champ "TP-OA".

Ainsi, lors de l'étape 54 de discrimination d'application 54, le module SIM identifie l'application distante émettrice du message en s'assurant que l'adresse TP-OA du message est identique à l'une des adresses TP-OA du fichier élémentaire d'entrée 60.

La figure 6 illustre également le fait que, pour chaque adresse TP-OA (c'est-à-dire

chaque application distante autorisée) du fichier élémentaire d'entrée 60, le module SIM a la possibilité d'accéder, dans la mémoire de données 8, à un ensemble 61 à 63 de trois paramètres : une référence secrète (Kappli), un mode d'authentification de message (algo_id) et un schéma sécuritaire.

Ainsi, comme illustré sur la figure 7, pour effectuer l'étape 57 d'authentification de message, le module SIM utilise la référence secrète (Kappli) et le mode d'authentification de message (algo_id) qui sont associés à l'application émettrice du message et qu'il a préalablement retrouvés dans la mémoire de données 8. A partir de ces deux paramètres (Kappli et algo_id) et des données du corp du message, le module SIM calcule par exemple un cryptogramme qui doit être identique à un cryptogramme (SMS-Cert) contenu dans le corp du message (cf figure 2) pour que l'authentification du message soit réussie.

La figure 8 permet d'expliciter l'étape 511 de sécurisation de l'exécution d'une commande. Chaque commande (ou opération) d'un message est effectivement éxécutée seulement si, d'après l'état courant de sécurité du module SIM ainsi que les informations et les attributs de sécurité liés à l'application distante émettrice du message, cette commande est autorisée à accéder aux fichiers sur lesquels elle travaille. Ceci correspond au schéma sécuritaire de l'application distante.

Dans la suite de la description, on présente un mode de réalisation particulier de l'invention, dans lequel chaque application distante autorisée est associée à un fichier élémentaire système (EF SMS System) de la mémoire de données 8.

Chaque fichier élémentaire système stocke une première information permettant de localiser dans la mémoire de données 8 un couple (référence secrète Kappli, mode d'authentification de message algo_id), ce couple étant associé à l'application distante autorisée à laquelle est lié ce fichier élémentaire système.

Dans le présent mode de réalisation, cette première information de localisation d'un couple (Kappli, algo_id) est un identificateur d'un fichier spécialisé sous lequel se trouve le fichier EF key_op contenant ce couple. Le fichier EF key_op peut stocker lui-même le mode d'authentification de message ou bien seulement un pointeur algo_id indiquant le lieu de stockage de ce mode d'authentification de message.

Par ailleurs, chaque message court amélioré comprend une seconde information de localisation du fichier élémentaire système auquel est liée l'application distante autorisée émettrice du message court amélioré.

Comme présenté sur la figure 2, dans le présent mode de réalisation, cette seconde information de localisation d'un fichier élémentaire système est un identificateur "DF entrée" (ou Login DF en langue anglaise) d'un fichier spécialisé ou d'un fichier maître auquel se rapporte, selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données, ce fichier élémentaire système.

Le module SIM met par exemple en oeuvre un mécanisme de recherche en amont (du type "backtracking"), consistant :

- à rechercher un fichier élémentaire système tout d'abord sous le fichier spécialisé ou le fichier maître courant (c'est-à-dire celui indiqué par l'identificateur "DF entrée"),
- puis, si aucun fichier élémentaire système n'existe sous le fichier spécialisé ou le fichier maître courant et si l'identificateur "DF entrée" n'indique pas le fichier maître, à rechercher un fichier élémentaire système directement sous le fichier maître.

Ainsi, le module SIM lit dans chaque message court amélioré filtré l'identificateur DF Id. A partir de cet identificateur "DF entrée", il retrouve le fichier élémentaire système auquel est liée l'application distante autorisée émettrice du message. Le module SIM lit dans ce fichier élémentaire système l'identificateur du fichier spécialisé sous lequel se trouve le fichier EF key_op. Dans ce fichier EF key_op, il lit le couple (Kappli, algo_id), de façon à connaître la référence secrète et le mode d'authentification de message à utiliser pour authentifier le message court amélioré filtré.

Un fichier élémentaire système au maximum peut être placé sous un fichier spécialisé. De même, un fichier élémentaire système au maximum peut être placé directement sous le fichier maître.

Si aucun fichier élémentaire système n'existe sous un fichier spécialisé, ni sous le fichier maître, les EF placés sous ce fichier spécialisé, quelle que soit la valeur de la condition d'accès à distance associée à chacun de ces fichiers élémentaires, ne sont

accessibles par aucune commande distante.

De même, si aucun fichier élémentaire système n'existe directement ni sous le fichier maître, alors les fichiers élémentaires placés directement sous le fichier maître, quelle que soit la valeur de la condition d'accès à distance associée à chacun de ces fichiers élémentaires, ne sont accessibles par aucune commande distante.

Dans le cas d'un fichier dont la condition d'accès à distance possède la valeur "PRIVE" ("accès privé"), l'unique application distante dont les commandes distantes peuvent accéder à ce fichier est, sous réserve que son authentification soit réussie, l'application distante autorisée liée au même fichier élémentaire système que celui auquel se rapporte le fichier spécialisé ou fichier maître parent de ce fichier. Cette application distante autorisée est dite parente de ce fichier.

Dans le cas d'un fichier dont la condition d'accès à distance possède la valeur "PARTAGE" ("accès partagé"), les applications distantes prédéterminées dont les commandes distantes peuvent accéder à ce fichier sont, sous réserve que leur authentification soit réussie, toutes les applications distantes autorisées, quel que soit le fichier élémentaire système auquel chacune d'elles est liée.

La figure 9 présente un exemple de mémoire de données 8 partagée entre deux applications distantes, à savoir :

- l'application "DF1", dont l'EF SMS System 91 se rapporte au fichier spécialisé DF1 ; et
- l'application "MF", dont le fichier élémentaire système 92 se rapporte au fichier maître MF.

On notera que les messages émis par l'application "DF1" comportent dans leur champ "DF entrée" la valeur DF1, qui est le fichier spécialisé sous lequel se trouve le fichier élémentaire système 91 de cette application "DF1".

Par contre, les messages émis par l'application "MF" comportent dans leur champ "DF entrée" la valeur MF/DF2, et non pas la valeur MF. En fait, aucun fichier élémentaire système ne se trouvant sous ce fichier spécialisé DF2, c'est bien sous le fichier maître que le module SIM va chercher (mécanisme de "backtracking") le fichier élémentaire système 92 de cette application "MF".

Dans cet exemple, on distingue les quatre groupes de fichiers suivants :

- groupe A' : les fichiers (DF1, EF2) uniquement accessibles par les commandes de l'application distante "DF1", c'est-à-dire les fichiers dont la condition d'accès à distance est "PRIVE" pour l'application "DF1" ;
- groupe B' : les fichiers (MF, DF2, EF5, EF7) uniquement accessibles par les commandes de l'application distante "MF" ;
- groupe C' : les fichiers (EF3, EF1, EF6) accessibles par les commandes des applications distantes "DF1" et "MF", c'est-à-dire les fichiers dont la condition d'accès à distance est "PARTAGE" pour les applications "DF1" et "MF" ;
- groupe D' : les fichiers (EF4) accessibles par les commandes d'aucune application distante, c'est-à-dire les fichiers dont la condition d'accès à distance est "JAMAIS".

Il est important de souligner que la présente invention permet, par l'intermédiaire de commandes distantes, de créer, mettre à jour ou encore supprimer certains éléments évoqués ci-dessus, tels que notamment :

- les valeurs des conditions d'accès, standard ou à distance, des politiques de contrôle d'accès associées à chaque fichier ;
- l'indicateur de la politique de contrôle d'accès, standard ou à distance, à utiliser avec chaque application pour chaque fichier ;
- la liste des applications distantes autorisées ;
- pour chacune des applications distantes autorisées, la référence secrète et le mode d'authentification de message associés ;
- les fichiers élémentaires systèmes EF SMS System liés chacun à une application distante autorisée distincte ;
- les fichiers élémentaires EF, spécialisés DF et maîtres MF.

La figure 10 présente un second exemple de partition de la mémoire de données 8. Dans ce second exemple, la mémoire de données 8 est partagée entre quatre applications distantes, à savoir :

- l'application "MF", dont le fichier élémentaire système EF SMS System 0

présente une sécurité activée, se rapporte au fichier maître ;

- l'application "DF1", dont le fichier élémentaire système EF SMS System 1 présente une sécurité désactivée, se rapporte au fichier spécialisé DF1 ;
- l'application "DF2", dont le fichier élémentaire système EF SMS System 2 présente une sécurité activée, se rapporte au fichier spécialisé DF2 ; et
- l'application "DF4", dont le fichier élémentaire système EF SMS System 4 présente une sécurité désactivée, se rapporte au fichier spécialisé DF4.

On entend par sécurité activée, pour un fichier élémentaire système, le fait que l'indicateur de politique de contrôle d'accès contenu dans ce fichier élémentaire système prévoit l'utilisation d'une politique de contrôle d'accès à distance. De même, on entend par sécurité désactivée, pour un fichier élémentaire système, le fait que l'indicateur de politique de contrôle d'accès contenu dans ce fichier élémentaire système prévoit l'utilisation de la politique de contrôle d'accès standard.

Il est à noter que le fichier spécialisé DF3, ainsi que tous les fichiers placés sous le fichier spécialisé DF3, ont pour application parente "MF" puisqu'il n'existe aucun fichier élémentaire système sous le fichier spécialisé DF3.

Chaque fichier élémentaire est associé à une valeur de condition d'accès à distance ("jamais", "privé", ou "partagé").

Le tableau de l'annexe 2 résume les différentes situations d'accès (accès autorisé ou refusé) pour chaque fichier élémentaire de la figure 10, en fonction du fichier spécialisé (ou fichier maître) spécifié dans l'en-tête du message.

Pour chaque fichier élémentaire à accéder par la commande (première colonne), on a indiqué:

- la valeur de condition d'accès à distance associée à ce fichier (première colonne également) ;
- l'EF ESMS System auquel se rapporte le fichier à accéder (seconde colonne) ; et
- l'état (activé ou désactivé) de la sécurité de cet EF ESMS System (seconde colonne également).

Pour chaque fichier spécialisé (ou fichier maître) spécifié dans l'en-tête du

message, on a indiqué le fichier spécialisé (ou fichier maître) parent du fichier élémentaire système où est effectuée l'authentification de message. On notera qu'aucune authentification de message n'est effectuée pour les fichiers spécialisés DF1 et DF4, dont les fichiers élémentaires systèmes (1 et 4 respectivement) présentent chacun une sécurité désactivée.

Ce tableau montre clairement que :

- si un fichier élémentaire système existe dans un fichier spécialisé, un fichier élémentaire de ce fichier spécialisé dont la condition d'accès à distance est "PRIVE" ne peut pas être accédé à travers une commande distante contenue dans un message authentifié dans un autre fichier spécialisé ;
- si aucun fichier élémentaire système n'existe dans un fichier spécialisé mais existe dans le fichier maître, un fichier élémentaire de ce fichier spécialisé dont la condition d'accès à distance est "PRIVE" ne peut pas être accédé à travers une commande distante contenue dans un message authentifié dans un autre fichier spécialisé, différent du fichier maître et contenant lui-même un fichier élémentaire système ;
- si aucun fichier élémentaire système n'existe dans un fichier spécialisé, ni dans le fichier maître, aucun message ne peut être authentifié sous ce fichier spécialisé et un fichier élémentaire de ce fichier spécialisé, quelle que soit sa condition d'accès à distance, ne peut pas être accédé à travers une commande distante (en d'autres termes, si aucun fichier élémentaire système n'est attaché à un fichier, tout accès à distance - à travers une commande distante - est interdit) ;
- dans tous les cas, un fichier élémentaire dont la condition d'accès à distance est "PARTAGE" peut être accédé à travers une commande distante contenue dans un message qui a été authentifié.

Ci-dessous, dans un but de simplification, on note :

- "LA" (pour "Login Appli" en langue anglaise) le fichier élémentaire système qui se rapporte au fichier spécialisé DF spécifié dans l'en-tête du message, et
- "PA" (pour "Parent Appli" en langue anglaise) le fichier élémentaire

système qui se rapporte au fichier à accéder.

La sécurité peut alors, d'une façon plus générale, être entièrement et formellement décrite avec les sept règles suivantes :

- R1. Si aucun fichier PA ne peut être trouvé,
  -> Alors l'accès à distance est interdit.
- R2. Si un fichier PA est trouvé, mais la condition d'accès à distance du fichier à accéder est "PRIVE" :
  -> Alors l'accès à distance est interdit.
- R3. Si un fichier PA est trouvé, et la condition d'accès à distance du fichier à accéder est "PRIVE", et le fichier PA n'est pas le même que le fichier LA :
  -> Alors l'accès à distance est interdit.
- R4. Si un fichier PA est trouvé, et la condition d'accès à distance du fichier à accéder est "PRIVE", et le fichier PA est le même que le fichier LA, et la sécurité est désactivée dans le fichier LA :
  -> Alors l'accès à distance dépend des conditions d'accès standard au fichier.
- R5. Si un fichier PA est trouvé, et la condition d'accès à distance du fichier à accéder est "PRIVE", et le fichier PA est le même que le fichier LA, et la sécurité est activée dans le fichier LA :
  -> Alors l'accès à distance est autorisé.
- R6. Si un fichier PA est trouvé, et la condition d'accès à distance du fichier à accéder est "PARTAGE", et la sécurité est désactivée dans le fichier LA :
  -> Alors l'accès à distance dépend des conditions d'accès standard au fichier.
- R7. Si un fichier PA est trouvé, et la condition d'accès à distance du fichier à accéder est "PARTAGE", et la sécurité est activée dans le fichier LA :
  -> Alors l'accès à distance est autorisé.

Annexe 1

Politique de contrôle d'accès(PCA)	Application	Commande	Condition d'accès	Valeur de la condition d'accès
PCA Standard	indifférent	commande (dist ou loc) 1	cond. d'acc std 1	ALWAYS
	indifférent	commande (dist ou loc) 2	cond. d'acc std 2	CHV1
	⋮	⋮	⋮	⋮
	indifférent	commande (dist ou loc) k	cond. d'acc std k	NEVER
PCA à distance N°1	appli. distante 1	commande dist. 1	condition d'accès à distance 1	PARTAGE
		commande dist. 2		
		⋮		
		commande dist. m		
	appli. distante 1'	commande dist. 1'		
		commande dist. 2'		
		⋮		
		commande dist. m'		
	appli. distante 1"	commande dist. 1"		
		commande dist. 2"		
		⋮		
		commande dist. m"		
	⋮			
PCA à distance N°2	appli. distante 1	commande dist. 1	condition d'accès à distance 2	X
		commande dist. 2		
		⋮		
		commande dist. m		
	appli. distante 1'	commande dist. 1'		
		commande dist. 2'		
		⋮		
		commande dist. m'		
	appli. distante 1"	commande dist. 1"		
		commande dist. 2"		
		⋮		
		commande dist. m"		
	⋮			

Annexe 2

		DF spécifié dans l'en-tête ESMS				
		MF	DF 2	DF 3	DF 1	DF 4
Fichier à accéder/ conditions d'accès à distance	EF SMS Système concerné	DF parent de l'EF SMS Syst. où est effectuée l'authentification de message			pas d'authen-tification de message	
		MF	DF 2	MF		
EF 01 (MF) privé	EF SMS Syst 0 (MF) Sécu activée	autorisé	refusé	autorisé	refusé	refusé
EF 02 (MF) partagé	EF SMS Syst 0 (MF) Sécu activée	autorisé	autorisé	autorisé	*	*
EF 03 (MF) jamais	EF SMS Syst 0 (MF) Sécu activée	refusé	refusé	refusé	refusé	refusé
EF 11 (DF 1) privé	EF SMS Syst 1 (DF 1) Sécu désactivée	refusé	refusé	refusé	*	refusé
EF 12 (DF 1) partagé	EF SMS Syst 1 (DF 1) Sécu désactivée	autorisé	autorisé	autorisé	*	*
EF 13 (DF 1) jamais	EF SMS Syst 1 (DF 1) Sécu désactivée	refusé	refusé	refusé	refusé	refusé
EF 21 (DF 2) privé	EF SMS Syst 2 (DF 2) Sécu activée	refusé	autorisé	refusé	refusé	refusé
EF 22 (DF 2) partagé	EF SMS Syst 2 (DF 2) Sécu activée	autorisé	autorisé	autorisé	*	*
EF 23 (DF 2) jamais	EF SMS Syst 2 (DF 2) Sécu activée	refusé	refusé	refusé	refusé	refusé
EF 31 (DF 3) privé	EF SMS Syst 0 (MF) Sécu activée	autorisé	refusé	autorisé	refusé	refusé
EF 32 (DF 3) partagé	EF SMS Syst 0 (MF) Sécu activée	autorisé	autorisé	autorisé	*	*
EF 33 (DF 3) jamais	EF SMS Syst 0 (MF) Sécu activée	refusé	refusé	refusé	refusé	refusé
EF 41 (DF 4) privé	EF SMS Syst 4 (DF 4) Sécu désactivée	refusé	refusé	refusé	refusé	*
EF 42 (DF 4) partagé	EF SMS Syst 4 (DF 4) Sécu désactivée	autorisé	autorisé	autorisé	*	*
EF 43 (DF 4) jamais	EF SMS Syst 4 (DF 4) Sécu désactivée	refusé	refusé	refusé	refusé	refusé

* = autorisé si condition d'accès standard remplie

REVENDICATIONS

1. Système de communication, du type comprenant notamment une pluralité d'équipements terminaux (MS ; 1) constitués chacun d'un terminal (ME ; 4) coopérant avec une carte utilisateur à microprocesseur (module SIM ; 5),

chaque carte utilisateur incluant des moyens (8) de mémorisation de données comprenant une pluralité d'objets (MF, DF, EF), lesdits moyens (8) de mémorisation de données servant de support à au moins deux applications distinctes (appli. GSM, appli. dist. 1 à appli. dist. 1'' ; Fidélité, Paiement, GSM ; "DF1", "MF"), ladite carte utilisateur comprenant des moyens (6, 7) d'exécution de commandes appartenant auxdites applications,

chaque objet compris dans les moyens de mémorisation de données d'une carte utilisateur étant associé à une première politique de contrôle d'accès (PCA Standard) définie par un jeu de premières conditions d'accès (cond. d'acc. std 1 à cond. d'acc. std k), chacune desdites premières conditions d'accès s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite première politique de contrôle d'accès,

caractérisé en ce que chaque objet est également associé à au moins une autre politique de contrôle d'accès (PCA à distance n°1, PCA à distance n°2), chaque autre politique de contrôle d'accès étant définie par un jeu d'au moins une condition d'accès alternative (cond. d'acc. à dist. 1, cond. d'acc. à dist. 2), chaque condition d'accès alternative d'une autre politique de contrôle d'accès donnée s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite autre politique de contrôle d'accès donnée,

et en ce que chaque objet est également associé à une pluralité d'indicateurs de politique de contrôle d'accès, chaque indicateur de politique de contrôle d'accès indiquant, pour une desdites applications, quelle politique de contrôle d'accès, à savoir première ou autre, utiliser avec cette application, lesdits indicateurs de politique de contrôle d'accès étant stockés dans lesdits moyens (8) de mémorisation de données.

2. Système selon la revendication 1, caractérisé en ce que, pour chaque objet, au moins une autre politique de contrôle d'accès est spécifique à une des applications,

chaque condition d'accès alternative de cette autre politique de contrôle d'accès spécifique s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à l'unique application utilisant cette autre politique de contrôle d'accès spécifique.

3. Système selon l'une quelconque des revendications 1 et 2, caractérisé en ce que, pour chaque objet, au moins une autre politique de contrôle d'accès est entièrement commune à au moins deux applications, chaque condition d'accès alternative de cette autre politique de contrôle d'accès entièrement commune s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant auxdites au moins deux applications utilisant cette autre politique de contrôle d'accès entièrement commune.

4. Système selon l'une quelconque des revendications 1 à 3, caractérisé en ce que, pour chaque objet, au moins une autre politique de contrôle d'accès est partiellement commune à au moins deux applications,

certaines des conditions d'accès alternatives de cette autre politique de contrôle d'accès partiellement commune s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant auxdites au moins deux applications utilisant cette autre politique de contrôle d'accès commune,

d'autres des conditions d'accès alternatives de cette autre politique de contrôle d'accès partiellement commune s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant uniquement à l'une desdites au moins deux applications utilisant cette autre politique de contrôle d'accès commune.

5. Système selon l'une quelconque des revendications 1 à 4, du type permettant une radiocommunication cellulaire, caractérisé en ce que ladite pluralité d'équipements terminaux est une pluralité de stations mobiles (MS ; 1), lesdites cartes utilisateur étant des modules d'identification d'abonné (module SIM ; 5).

6. Système selon l'une quelconque des revendications 1 à 5, du type comprenant en outre au moins un centre de service de messages (C-SMS),

lesdits moyens de mémorisation de données d'une carte utilisateur servant de support à au moins une application locale et au moins une application distante de ladite carte utilisateur, les commandes étant dites locales, lorsqu'elles appartiennent à ladite application locale, ou distantes, lorsqu'elles appartiennent à ladite application distante,

chaque terminal (4) pouvant recevoir des messages, de type normal (SMS) ou amélioré (ESMS), émis par ledit centre de service de messages, chaque carte utilisateur (5) comprenant des moyens (9) de stockage et de traitement des messages reçus par le terminal avec lequel elle coopère,

les messages normaux contenant des données brutes constituant une information destinée à être fournie à l'abonné via notamment un écran d'affichage du terminal, les messages améliorés (20) contenant des commandes distantes (cmd 1, cmd 2, ...),

caractérisé en ce que lesdits moyens (8) de mémorisation de données de chaque carte utilisateur stockent également une liste d'applications distantes autorisées (TP-OA 1 à TP-OA n),

et en ce que chaque carte utilisateur comprend également des moyens de discrimination des messages améliorés, permettant de bloquer chaque message amélioré qui contient des commandes distantes n'appartenant pas à une desdites applications distantes autorisées.

7. Système selon la revendication 6, caractérisé en ce que lesdits moyens de mémorisation de données de chaque carte utilisateur stockent également, pour chacune desdites applications distantes autorisées, une référence secrète (Kappli) et un mode d'authentification de message (algo_id) associés,

et en ce que chaque carte utilisateur (module SIM) comprend également des moyens d'authentification des messages améliorés discriminés, permettant d'authentifier un message amélioré discriminé en utilisant la référence secrète et le mode d'authentification de message associés, dans lesdits moyens de mémorisation de données, à l'application distante autorisée à laquelle appartiennent les commandes contenues dans ledit message amélioré discriminé.

8. Système selon l'une quelconque des revendications 1 à 7, caractérisé en ce que, pour chaque objet, la ou au moins une des autres politiques de contrôle d'accès, dite seconde politique de contrôle d'accès, est définie par un jeu d'au moins une condition d'accès alternative particulière, chaque condition d'accès alternative particulière pouvant prendre notamment les valeurs suivantes :

- "aucun accès" ("JAMAIS") : si ledit objet n'est accessible par aucune

commande dudit groupe d'au moins une commande auquel s'applique ladite condition d'accès alternative particulière ;

- "accès privé" ("PRIVE") : si ledit objet n'est accessible que par les commandes appartenant à une unique application prédéterminée, parmi ledit groupe d'au moins une commande auquel s'applique ladite condition d'accès alternative particulière ;
- "accès partagé" ("PARTAGE") : si ledit objet est accessible par les commandes appartenant à au moins deux applications prédéterminées, parmi ledit groupe d'au moins une commande auquel s'applique ladite condition d'accès alternative particulière.

9. Système selon l'une quelconque des revendications 6 à 8, caractérisé en ce que, pour chaque objet, au moins une autre politique de contrôle d'accès, dite politique de contrôle d'accès à distance, est définie par un jeu d'au moins une condition d'accès à distance (cond. d'acc. à dist. 1, cond. d'acc. à dist. 2), chaque condition d'accès à distance s'appliquant, pour ledit objet, à un groupe d'au moins une commande distante appartenant à la ou aux applications distantes utilisant ladite politique de contrôle d'accès à distance,

et en ce que, pour chaque objet, seuls les indicateurs de politique de contrôle d'accès associés chacun à une des applications distantes peuvent indiquer ladite politique de contrôle d'accès à distance.

10. Système selon les revendications 8 et 9, caractérisé en ce que, pour chaque objet, chaque condition d'accès à distance peut prendre les mêmes valeurs ("JAMAIS", "PRIVE", "PARTAGE") que lesdites conditions d'accès alternatives particulières.

11. Système selon l'une quelconque des revendications 7 à 10, lesdits moyens de mémorisation de données de chaque carte utilisateur possèdant une structure hiérarchique à au moins trois niveaux et comprenant au moins les trois types de fichiers suivants :

- fichier maître (MF), ou répertoire principal ;
- fichier spécialisé (DF), ou répertoire secondaire placé sous ledit fichier maître ;
- fichier élémentaire (EF), placé sous un desdits fichiers spécialisés, dit

fichier spécialisé parent, ou directement sous ledit fichier maître, dit fichier maître parent,

caractérisé en ce que lesdits moyens de mémorisation de données de chaque carte utilisateur comprennent au moins un fichier élémentaire système (EF SMS System), chaque fichier élémentaire système étant lié à une application distante autorisée et stockant une première information de localisation de la référence secrète et du mode d'authentification de message associés à cette application distante autorisée à laquelle il est lié,

et en ce que chaque message amélioré comprend une seconde information ("DF entrée") de localisation du fichier élémentaire système auquel est liée l'application distante autorisée à laquelle appartiennent les commandes contenues dans ledit message amélioré,

lesdits moyens d'authentification lisant dans chaque message amélioré discriminé ladite seconde information de localisation du fichier élémentaire système, de façon à lire dans le fichier élémentaire système ladite première information de localisation de la référence secrète et du mode d'authentification de message à utiliser pour authentifier ledit message amélioré discriminé.

12. Système selon la revendication 11, caractérisé en ce que chaque fichier élémentaire système (EF SMS System) est placé sous un fichier spécialisé (DF) ou directement sous le fichier maître (MF), un fichier élémentaire système au maximum pouvant être placé sous chaque fichier spécialisé, et un fichier élémentaire système au maximum pouvant être placé directement sous le fichier maître.

13. Système selon la revendication 12, caractérisé en ce que si aucun fichier élémentaire système (EF SMS System) n'existe sous un fichier spécialisé (DF), ni sous le fichier maître (MF), alors chaque fichier élémentaire (EF) placé sous ledit fichier spécialisé, quelle que soit la valeur des conditions d'accès à distance associées à ce fichier élémentaire, n'est accessible par aucune commande distante,

et en ce que si aucun fichier élémentaire système (EF SMS System) n'existe directement sous le fichier maître (MF), alors chaque fichier élémentaire (EF) placé directement sous le fichier maître, quelle que soit la valeur des conditions d'accès à distance associées à ce fichier élémentaire, n'est accessible par aucune commande

distante.

14. Système selon l'une quelconque des revendications 11 à 13, caractérisé en ce que ladite seconde information de localisation du fichier élémentaire système (EF SMS System) est un identificateur ("DF entrée") d'un fichier spécialisé (DF) ou d'un fichier maître (MF) auquel se rapporte ledit fichier élémentaire système selon une stratégie de recherche prédéterminée dans les moyens de mémorisation de données.

15. Système selon la revendication 14, caractérisé en ce que ladite stratégie de recherche prédéterminée dans les moyens de mémorisation de données est un mécanisme de recherche en amont (du type "backtracking"), consistant à rechercher si un fichier élémentaire système (EF SMS System) existe sous le fichier spécialisé (DF) ou le fichier maître (MF) indiqué par ledit identificateur, et, dans la négative et si l'identificateur n'indique pas le fichier maître, à rechercher si un fichier élémentaire système existe directement sous le fichier maître.

16. Système selon la revendication 10 et l'une quelconque des revendications 11 à 15, caractérisé en ce que, dans le cas d'un fichier dont une des conditions d'accès à distance possède la valeur "accès privé", ladite unique application distante prédéterminée dont les commandes distantes peuvent accéder audit fichier est, sous réserve que son authentification soit réussie, l'application distante autorisée parente dudit fichier, c'est-à-dire l'application distante autorisée liée au même fichier élémentaire système (EF SMS System) que celui auquel se rapporte le fichier spécialisé (DF) parent ou le fichier maître (MF) parent dudit fichier,

et en ce que, dans le cas d'un fichier dont la condition d'accès à distance possède la valeur "accès partagé", lesdites au moins deux applications distantes prédéterminées dont les commandes distantes peuvent accéder audit fichier sont, sous réserve que leur authentification soit réussie, toutes les applications distantes autorisées, quel que soit le fichier élémentaire système (EF SMS System) auquel chacune d'elles est liée.

17. Système selon l'une quelconque des revendications 11 à 16, caractérisé en ce que chaque fichier élémentaire système (EF SMS System) comprend un ensemble distinct d'indicateurs de politique de contrôle d'accès, chaque indicateur de politique de contrôle d'accès indiquant, pour une desdites applications, quelle politique de contrôle d'accès, à

savoir première ou autre, utiliser avec cette application,

ledit ensemble distinct d'indicateurs de politique de contrôle d'accès étant associé à tous les fichiers (EF, DF, MF) dont le fichier spécialisé (DF) parent ou le fichier maître (MF) parent se rapporte audit fichier élémentaire système (EF SMS System).

18. Carte utilisateur à microprocesseur (module SIM) du type destiné à coopérer avec un terminal (ME ; 4) de façon à constituer un équipement terminal (MS ; 1) d'un système de communication selon l'une quelconque des revendications 1 à 17,

caractérisé en ce que chaque objet des moyens de mémorisation de données de ladite carte utilisateur est également associé à au moins une autre politique de contrôle d'accès (PCA à distance n°1, PCA à distance n°2), chaque autre politique de contrôle d'accès étant définie par un jeu d'au moins une condition d'accès alternative (cond. d'acc. à dist. 1, cond. d'acc. à dist. 2), chaque condition d'accès alternative d'une autre politique de contrôle d'accès donnée s'appliquant, pour ledit objet, à un groupe d'au moins une commande appartenant à la ou aux applications utilisant ladite autre politique de contrôle d'accès donnée,

et en ce que chaque objet est également associé à une pluralité d'indicateurs de politique de contrôle d'accès, chaque indicateur de politique de contrôle d'accès indiquant, pour une desdites applications, quelle politique de contrôle d'accès, à savoir première ou autre, utiliser avec cette application, lesdits indicateurs de politique de contrôle d'accès étant stockés dans les moyens (8) de mémorisation de données de ladite carte utilisateur.

19. Procédé de gestion sécurisée et indépendante d'au moins deux applications distantes, par une carte utilisateur à microprocesseur (module SIM ; 5) du type destiné à coopérer avec un terminal (ME ; 4) de façon à constituer un équipement terminal (MS ; 1) d'un système de communication selon l'une quelconque des revendications 6 à 17,

caractérisé en ce que, pour chaque message amélioré reçu, ladite carte utilisateur (module SIM) effectue notamment l'étape suivante (511) : pour chaque commande distante contenue dans ledit message amélioré, vérification de l'accessibilité de cette commande distante à l'objet concerné, ladite vérification de l'accessibilté s'appuyant sur une politique de contrôle d'accès, première ou à distance, à utiliser pour ledit objet

concerné avec ladite application distante courante.

20. Procédé selon la revendication 19, caractérisé en ce que, pour chaque message amélioré reçu, ladite carte utilisateur (module SIM) effectue également une étape préalable (54) de discrimination dudit message amélioré, de façon à ne poursuivre son traitement que si l'application distante, dite application distante courante, à laquelle appartiennent les commandes distantes qu'il contient est une application distante autorisée.

21. Procédé selon l'une quelconque des revendication 19 et 20, caractérisé en ce que, pour chaque message amélioré reçu, ladite carte utilisateur (module SIM) effectue également une étape préalable (57) d'authentification dudit message amélioré, en utilisant une référence secrète et un mode d'authentification de message associés à ladite application distante courante.

22. Procédé selon l'une quelconque des revendications 19 à 21, caractérisé en ce que au moins certains des éléments appartenant au groupe suivant peuvent être créés et/ou mis à jour et/ou supprimés par l'intermédiaire de commandes distantes :

- les valeurs des conditions d'accès, notamment premières ou à distance, des politiques de contrôle d'accès associées à chaque objet ;
- l'indicateur de politique de contrôle d'accès, notamment première ou à distance, à utiliser avec chaque application pour chaque objet ;
- la liste des applications distantes autorisées ;
- pour chacune des applications distantes autorisées de ladite liste, la référence secrète et le mode d'authentification de message associés ;
- le ou lesdits fichiers élémentaires systèmes (EF SMS System) liés chacun à une application distante autorisée distincte ;
- les fichiers élémentaires (EF), spécialisé (DF) et maître (MF).

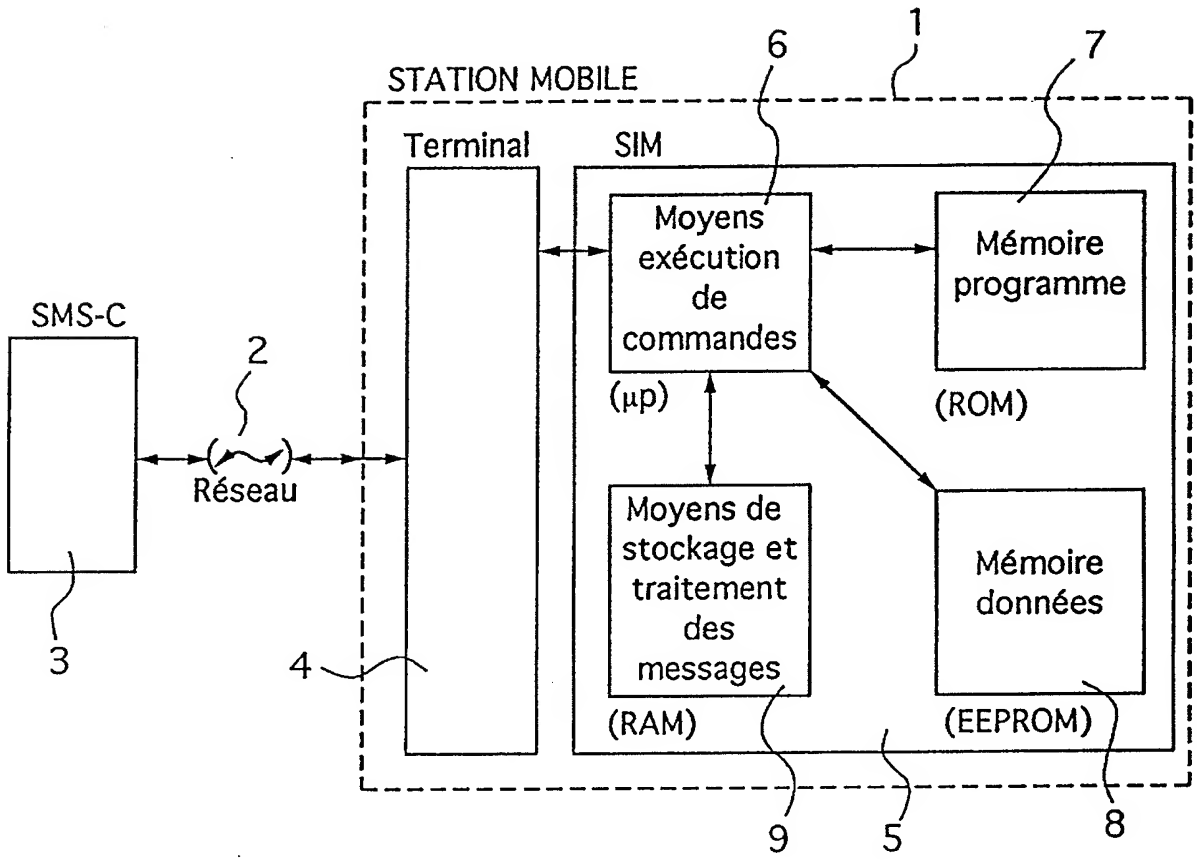

STATION MOBILE
1
6
7
Terminal
SIM
Moyens exécution de commandes
(µp)
Mémoire programme
(ROM)
SMS-C
2
Réseau
3
4
Moyens de stockage et traitement des messages
(RAM)
Mémoire données
(EEPROM)
9
5
8

Fig. 1

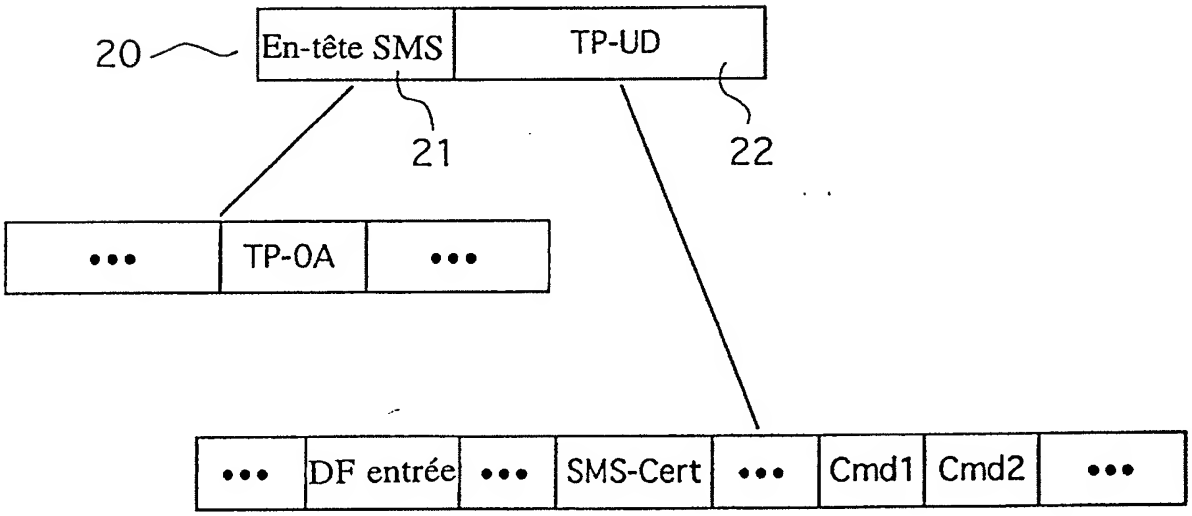

20
En-tête SMS
TP-UD
21
22
•••
TP-0A
•••
•••
DF entrée
•••
SMS-Cert
•••
Cmd1
Cmd2
•••

Fig. 2

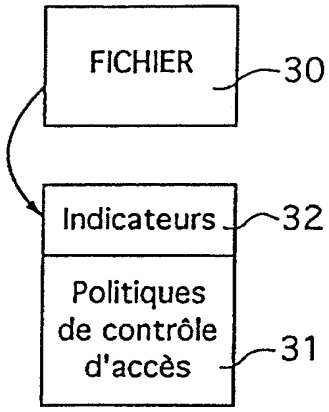


Fig. 3A

32

Application	Indicateurs de politique de contrôle d'accès
appli. GSM	PCA standard
appli. dist. 1	PCA à distance N°1
appli. dist. 1'	PCA standard
appli. dist. 1"	PCA à distance N°2
⋮	

Fig. 3B

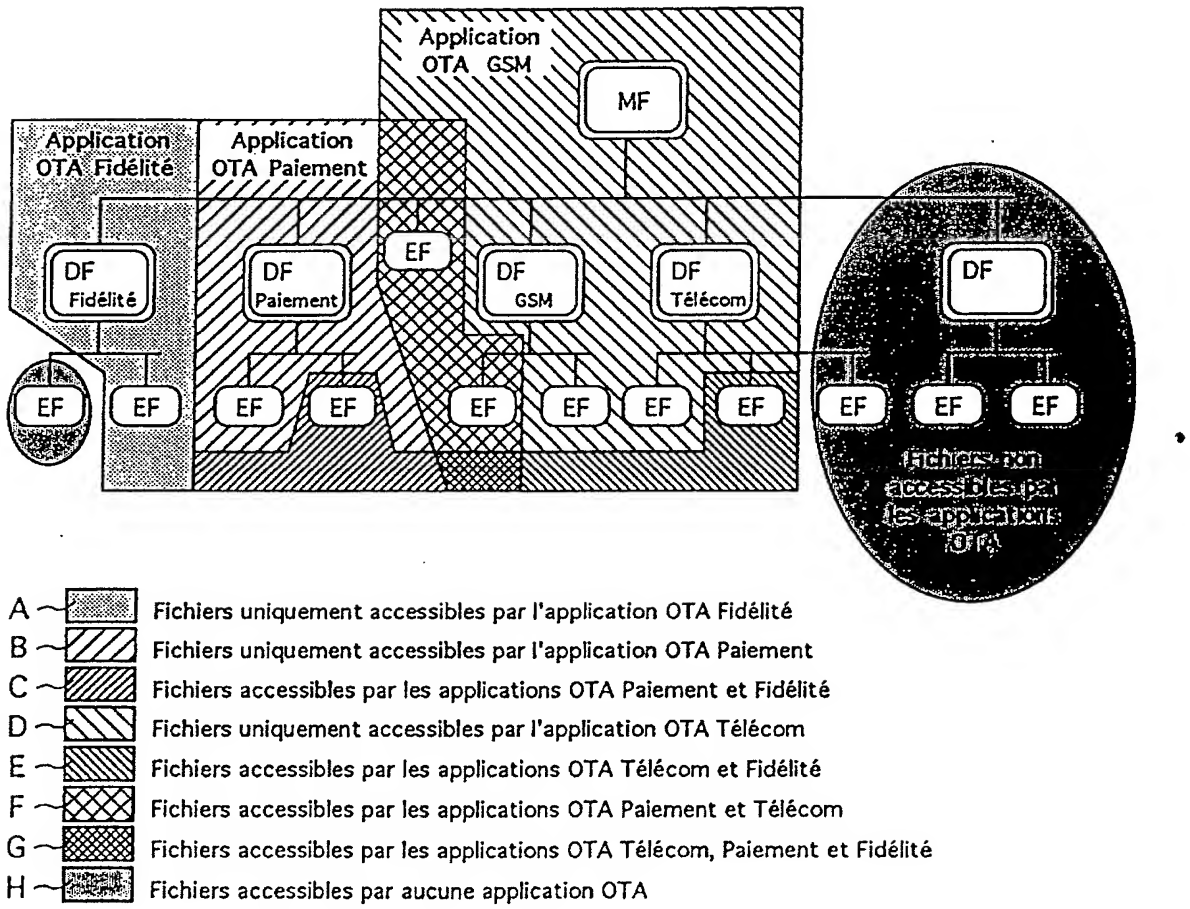


Fig. 4

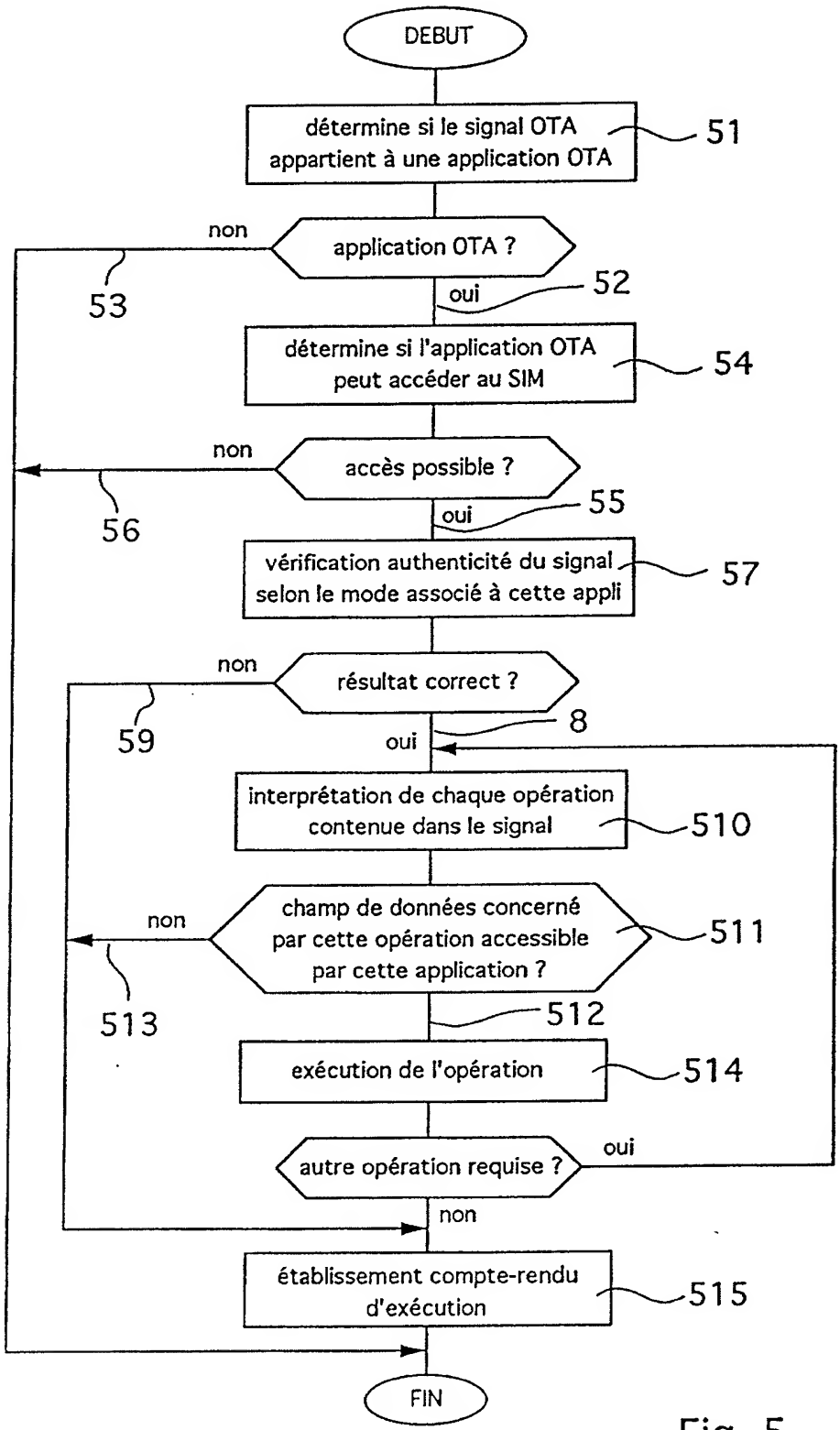

DEBUT
détermine si le signal OTA appartient à une application OTA
51
non
application OTA ?
53
oui
52
détermine si l'application OTA peut accéder au SIM
54
non
accès possible ?
56
oui
55
vérification authenticité du signal selon le mode associé à cette appli
57
non
résultat correct ?
59
oui
8
interprétation de chaque opération contenue dans le signal
510
non
champ de données concerné par cette opération accessible par cette application ?
511
513
512
exécution de l'opération
514
autre opération requise ?
oui
non
établissement compte-rendu d'exécution
515
FIN

Fig. 5

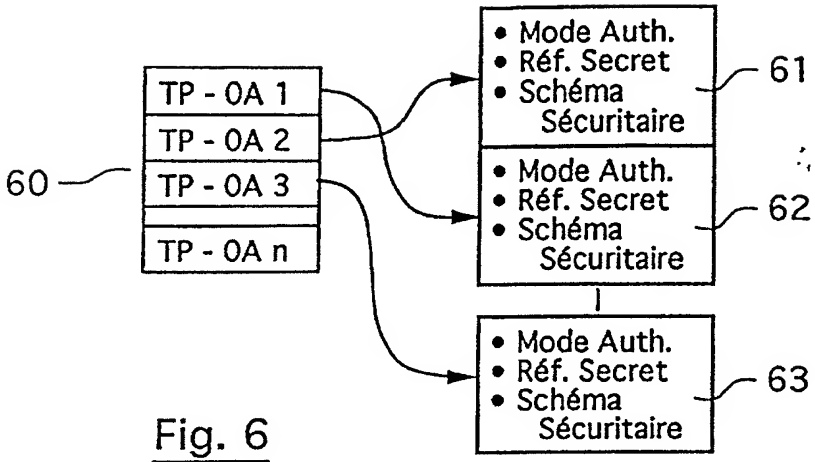


Fig. 6

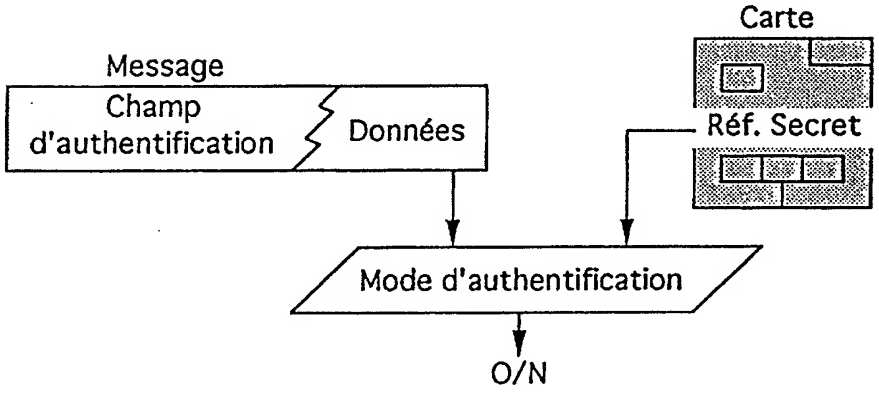


Fig. 7

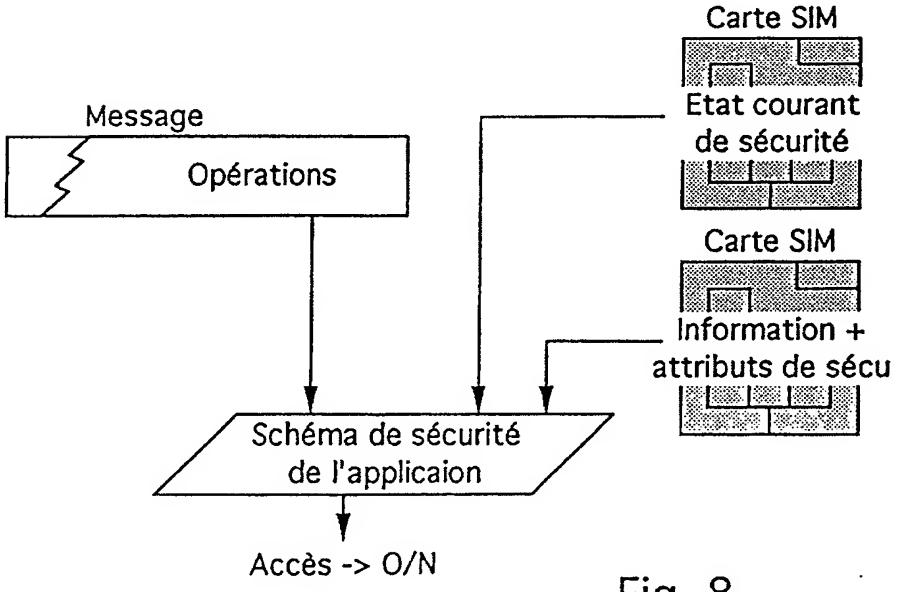


Fig. 8

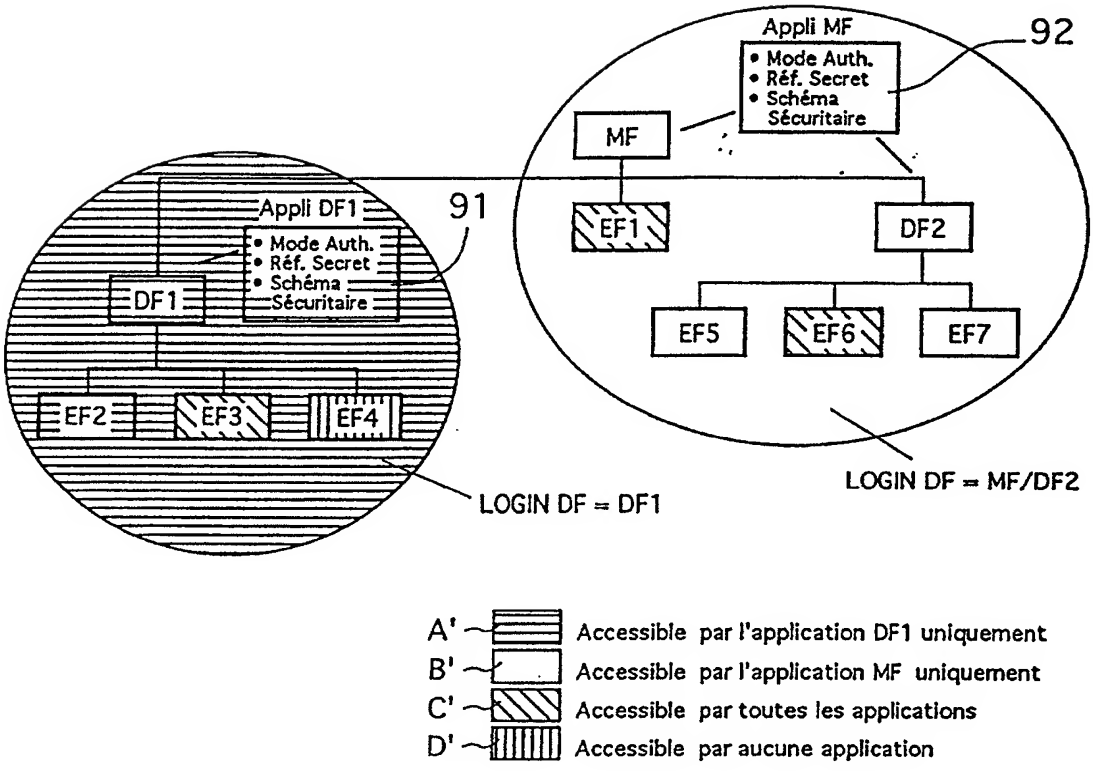

Appli MF
92
• Mode Auth.
• Réf. Secret
• Schéma Sécuritaire
MF
EF1
DF2
EF5
EF6
EF7
Appli DF1
91
• Mode Auth.
• Réf. Secret
• Schéma Sécuritaire
DF1
EF2
EF3
EF4
LOGIN DF = DF1
LOGIN DF = MF/DF2
A' Accessible par l'application DF1 uniquement
B' Accessible par l'application MF uniquement
C' Accessible par toutes les applications
D' Accessible par aucune application

Fig. 9

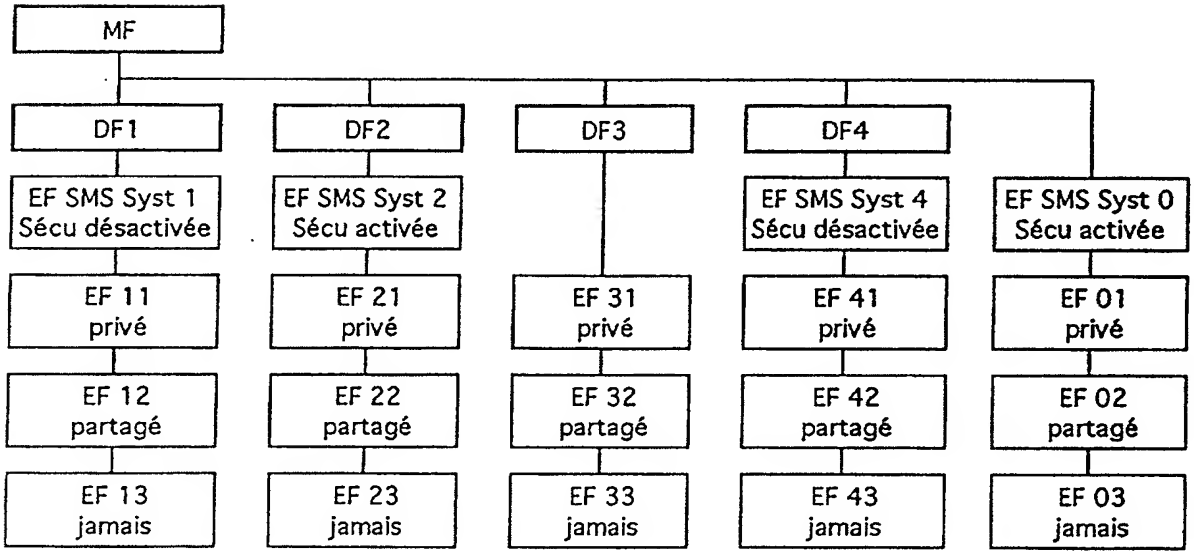

MF
DF1
DF2
DF3
DF4
EF SMS Syst 1 Sécu désactivée
EF SMS Syst 2 Sécu activée
EF SMS Syst 4 Sécu désactivée
EF SMS Syst 0 Sécu activée
EF 11 privé
EF 21 privé
EF 31 privé
EF 41 privé
EF 01 privé
EF 12 partagé
EF 22 partagé
EF 32 partagé
EF 42 partagé
EF 02 partagé
EF 13 jamais
EF 23 jamais
EF 33 jamais
EF 43 jamais
EF 03 jamais

Fig. 10

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2748834
N° d'enregistrement national

FA 528851
FR 9606382

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
X Y	EP 0 644 513 A (AT & T CORP) 22 Mars 1995 * colonne 2, ligne 11 - ligne 48 * * colonne 5, ligne 40 - colonne 7, ligne 25 * * colonne 9, ligne 19 - ligne 28 * * colonne 11, ligne 15 - ligne 22 * * colonne 12, ligne 12 - ligne 43 * * colonne 13, ligne 15 - colonne 13, ligne 50 * * colonne 16, ligne 15 - ligne 43 * * colonne 19, ligne 3 - ligne 42 * ---	1-5,18 6-17, 19-22
X Y	EP 0 666 550 A (JONG EDUARD KAREL DE) 9 Août 1995 * colonne 2, ligne 30 - colonne 3, ligne 20 * * colonne 3, ligne 48 - colonne 4, ligne 40 * * colonne 7, ligne 57 - colonne 8, ligne 9 * * colonne 11, ligne 28 - colonne 14, ligne 42 * * colonne 18, ligne 38 - colonne 21, ligne 24 * * colonne 23, ligne 21 - ligne 55 * ---	1-5, 8-10,18 6,7, 11-17, 19-22
Y,D	WO 94 30023 A (CELLTRACE COMMUNICATIONS LIMIT ;MICHAELS WAYNE DAVID (GB); TIMSON) 22 Décembre 1994 * page 3, ligne 6 - ligne 12 * * colonne 7, ligne 23 - colonne 9, ligne 30 * * colonne 10, ligne 10 - ligne 28 * --- -/--	6-17, 19-22

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)
G07F H04Q

1

Date d'achèvement de la recherche	Examinateur
10 Février 1997	Gerling, J.C.J.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2748834
N° d'enregistrement national

FA 528851
FR 9606382

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	PROCEEDINGS OF THE NORDIC SEMINAR ON DIGITAL LAND MOBILE RADIO COMMUNICATIONS (DMR), OSLO, JUNE 26 - 28, 1990, no. SEMINAR 4, 26 Juin 1990, GENERAL DIRECTORATE OF POSTS AND TELECOMMUNICATIONS;FINLAND, pages 3.1, 1-09, XP000515543 MAZZIOTTO G: "THE SUBSCRIBER IDENTITY MODULE FOR THE EUROPEAN DIGITAL CELLULAR SYSTEM GSM" * page 8, alinéa 3.3. - page 9, alinéa 4. * * page 9, ligne 34 - ligne 44 * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

Date d'achèvement de la recherche	Examinateur
10 Février 1997	Gerling, J.C.J.

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C13)